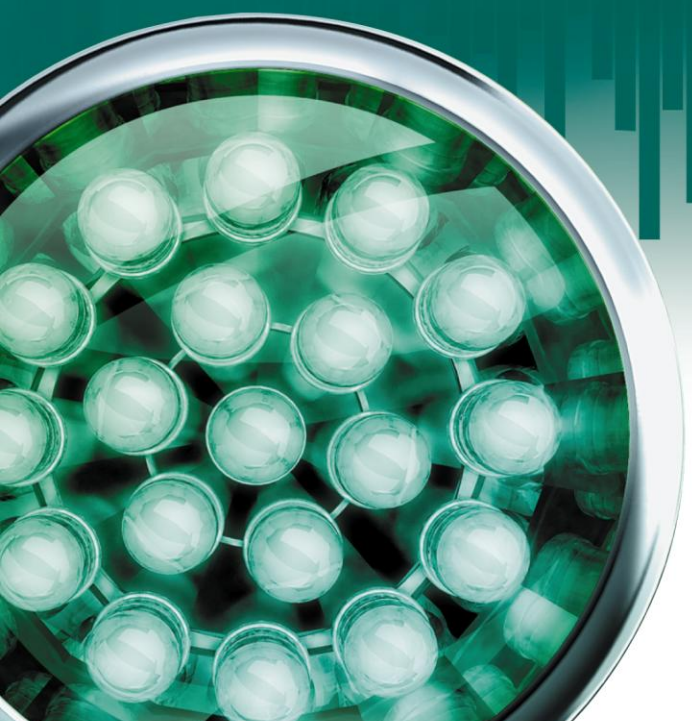
Kaspersky Mobile Security 9.0

GUIDA DELL'UTENTE

VERSIONE PROGRAMMA: 9.0



KASPERSKY lab

Gentile Utente!

Grazie per aver scelto il nostro prodotto. Ci auguriamo che questa documentazione possa essere di grande utilità nel lavoro e fornisca sempre risposte ad ogni domanda sul presente prodotto software.

La riproduzione o distribuzione di qualunque materiale in qualunque formato, incluse le traduzioni, è consentita previo consenso scritto di Kaspersky Lab.

Il presente documento e le immagini in esso contenute può essere utilizzato esclusivamente per scopi informativi non commerciali e personali.

Kaspersky Lab si riserva il diritto di modificare il presente documento senza ulteriore preavviso. È possibile reperire la versione più recente del presente documento sul sito Web di Kaspersky Lab all'indirizzo http://www.kaspersky.com/it/docs.

Kaspersky Lab non potrà essere ritenuta responsabile per il contenuto, qualità, pertinenza o accuratezza di qualunque materiale utilizzato nel presente documento i cui diritti sono di proprietà di terzi o per perdite potenzialo o effettive associate all'uso di tali materiali.

Nel presente documento sono utilizzati marchi registrati e marchi di servizio di proprietà dei detentori.

Data ultima revisione documento: 4 febbraio, 2010

© 2004–2010 Kaspersky Lab ZAO. Tutti i diritti riservati.

http://www.kaspersky.it/
http://www.kaspersky.com/it/service

SOMMARIO

CONTRATTO DI LICENZA CON L'UTENTE FINALE KASPERSKY LAB 8

KASPERSKY MOBILE SECURITY 9.0 13

Come ottenere informazioni sull'applicazione 14

Fonti di informazione per ulteriori ricerche 14

Come contattare l'Ufficio Vendite 15

Forum Web di discussione sulle applicazioni Kaspersky Lab 15

Novità di Kaspersky Mobile Security 9.0 15

Requisiti Hardware e Software 16

Kit di distribuzione 16

KASPERSKY MOBILE SECURITY 9.0 PER SISTEMA OPERATIVO SYMBIAN 17

Installazione di Kaspersky Mobile Security 9.0 17

Disinstallazione dell'applicazione 18

Aggiornamento dell'applicazione dalla versione 8.0 alla versione 9.0 21

Operazioni preliminari 22

Attivazione dell'applicazione 22

Immissione della password segreta 26

Avvio dell'applicazione 27

Aggiornamento dei database dell'applicazione 27

Scansione anti-virus del dispositivo 28

Visualizzazione di informazioni sull'applicazione 28

Gestione della licenza 28

Informazioni sul Contratto di licenza 29

Informazioni sulle licenze di Kaspersky Mobile Security 29

Informazioni sui file chiave di Kaspersky Mobile Security 29

Visualizzazione delle informazioni sulla licenza 30

Rinnovo della licenza 31

Interfaccia dell'applicazione 33

Icona Protezione 33

Finestra Stato di protezione 34

Schede dell'applicazione 35

Menu dell'applicazione 36

Protezione del file system 36

Informazioni sul componente Protezione 37

Abilitazione e disabilitazione del componente Protezione 37

Configurazione dell'area di protezione 38

Selezione dell'azione da eseguire sugli oggetti rilevati 39

Ripristino delle impostazioni di protezione predefinite 40

Scansione del dispositivo 40

Informazioni sulla scansione del dispositivo 41

Avvio di una scansione manuale 41

Avvio di una scansione pianificata 43

Selezione del tipo di oggetti da sottoporre a scansione 44

Selezione dell'azione da eseguire sugli oggetti rilevati 45

Configurazione della scansione degli archivi 47

Ripristino delle impostazioni predefinite di scansione del dispositivo 48

Quarantena degli oggetti potenzialmente infetti ... 48
Informazioni sulla Quarantena ... 49
Visualizzazione di oggetti in quarantena ... 49
Ripristino di oggetti dalla quarantena ... 50
Eliminazione di oggetti dalla quarantena ... 50
Filtro delle chiamate e dei messaggi SMS in entrata ... 50
Informazioni su Anti-Spam ... 51
Modalità Anti-Spam ... 52
Modifica della modalità Anti-Spam ... 52
Creazione di una Lista bloccati ... 53
Creazione di una Lista consentiti ... 56
Risposta ai messaggi SMS e alle chiamate da contatti non in rubrica ... 59
Risposta ai messaggi SMS da mittenti non numerici ... 60
Selezione di una risposta ai messaggi SMS in entrata ... 61
Selezione di una risposta alle chiamate in entrata ... 62
Limitazione delle chiamate e dei messaggi SMS in uscita. Parental Control ... 63
Informazioni su Parental Control ... 63
Modalità Parental Control ... 64
Modifica della modalità Parental Control ... 64
Creazione di una Lista bloccati ... 65
Creazione di una Lista consentiti ... 68
Protezione dei dati in caso di smarrimento o furto del dispositivo ... 71
Informazioni su Antifurto ... 72
Blocco del dispositivo ... 72
Eliminazione dei dati personali ... 74
Creazione di un elenco di oggetti da eliminare ... 76
Monitoraggio della sostituzione di una scheda SIM sul dispositivo ... 77
Determinazione delle coordinate geografiche del dispositivo ... 78
Avvio remoto delle funzioni di Antifurto ... 80
Mascheramento dei dati personali ... 81
Protezione privacy ... 82
Modalità di Protezione privacy ... 82
Modifica della modalità di Protezione privacy ... 82
Avvio automatico di Protezione privacy ... 83
Avvio remoto di Protezione privacy ... 84
Creazione di un elenco di contatti protetti ... 86
Selezione degli oggetti di protezione: Protezione privacy ... 88
Filtro dell'attività di rete. Firewall ... 89
Informazioni su Firewall ... 89
Livelli di sicurezza di Firewall ... 90
Selezione del livello di sicurezza di Firewall ... 90
Notifica del tentativo di connessione ... 91
Criptaggio dei dati personali ... 92
Informazioni sul componente Criptaggio ... 92
Criptaggio dei dati ... 93
Decriptaggio dei dati ... 94
Blocco dell'accesso ai dati criptati ... 95
Aggiornamento dei database dell'applicazione ... 96
Informazioni sull'aggiornamento dei database dell'applicazione ... 97

Visualizzazione delle informazioni sul database ... 97
Avvio di aggiornamenti manuale ... 98
Avvio di aggiornamenti pianificati ... 99
Aggiornamento in roaming ... 100
Configurazione delle impostazioni di connessione a Internet ... 101
Report dell'applicazione ... 102
Informazioni sui report ... 102
Visualizzazione dei record del report ... 103
Eliminazione dei record del report ... 103
Configurazione di impostazioni aggiuntive ... 104
Modifica della password segreta ... 104
Visualizzazione dei suggerimenti ... 104
Configurazione delle notifiche acustiche ... 105
Gestione della retroilluminazione ... 106
Visualizzazione della finestra di stato ... 106
Visualizzazione dell'icona Protezione ... 107
KASPERSKY MOBILE SECURITY 9.0 PER MICROSOFT WINDOWS MOBILE ... 109
Installazione di Kaspersky Mobile Security 9.0 ... 109
Disinstallazione dell'applicazione ... 110
Aggiornamento dalla versione 8.0 alla versione 9.0 ... 112
Operazioni preliminari ... 113
Attivazione dell'applicazione ... 113
Immissione della password segreta ... 116
Avvio dell'applicazione ... 117
Aggiornamento dei database dell'applicazione ... 117
Scansione anti-virus del dispositivo ... 118
Visualizzazione di informazioni sull'applicazione ... 118
Gestione della licenza ... 119
Interfaccia dell'applicazione ... 123
Finestra Stato di protezione ... 123
Menu dell'applicazione ... 125
Protezione del file system ... 126
Informazioni sul componente Protezione ... 127
Abilitazione e disabilitazione del componente Protezione ... 127
Selezione dell'azione da eseguire sugli oggetti rilevati ... 128
Scansione del dispositivo ... 129
Informazioni sulle scansioni manuali ... 130
Avvio di una scansione manuale ... 130
Avvio di una scansione pianificata ... 132
Selezione del tipo di oggetti da sottoporre a scansione ... 133
Configurazione della scansione degli archivi ... 134
Selezione dell'azione da eseguire sugli oggetti rilevati ... 135
Quarantena degli oggetti malware ... 136
Informazioni sulla Quarantena ... 136
Visualizzazione di oggetti in quarantena ... 137
Ripristino di oggetti dalla quarantena ... 137
Eliminazione di oggetti dalla quarantena ... 138
Filtro delle chiamate e dei messaggi SMS in entrata ... 138

Informazioni su Anti-Spam ... 139
Modalità Anti-Spam ... 140
Modifica della modalità Anti-Spam ... 140
Creazione di una Lista bloccati ... 141
Creazione di una Lista consentiti ... 144
Risposta ai messaggi SMS e alle chiamate da contatti non in rubrica ... 147
Risposta ai messaggi SMS da mittenti non numerici ... 148
Selezione di una risposta ai messaggi SMS in entrata ... 149
Selezione di una risposta alle chiamate in entrata ... 150
Limitazione delle chiamate e dei messaggi SMS in uscita. Parental Control ... 151
Informazioni su Parental Control ... 152
Modalità Parental Control ... 152
Abilitazione/disabilitazione di Parental Control ... 152
Creazione di una Lista bloccati ... 153
Creazione di una Lista consentiti ... 156
Protezione dei dati in caso di smarrimento o furto del dispositivo ... 159
Informazioni su Antifurto ... 160
Blocco del dispositivo ... 161
Eliminazione dei dati personali ... 162
Creazione di un elenco di dati eliminati ... 165
Monitoraggio della sostituzione di una scheda SIM sul dispositivo ... 166
Determinazione delle coordinate geografiche del dispositivo ... 167
Avvio remoto delle funzioni di Antifurto ... 169
Mascheramento dei dati personali ... 170
Protezione privacy ... 171
Modalità di Protezione privacy ... 171
Abilitazione/disabilitazione di Protezione privacy ... 172
Avvio automatico di Protezione privacy ... 173
Avvio remoto di Protezione privacy ... 174
Creazione di un elenco di contatti protetti ... 175
Selezione degli oggetti di protezione: Protezione privacy ... 178
Filtro dell'attività di rete. Firewall ... 179
Informazioni su Firewall ... 179
Abilitazione/disabilitazione di Firewall ... 180
Selezione del livello di sicurezza di Firewall ... 180
Criptaggio dei dati personali ... 181
Informazioni sul componente Criptaggio ... 181
Criptaggio dei dati ... 182
Decriptaggio dei dati ... 183
Blocco dell'accesso ai dati criptati ... 184
Aggiornamento dei database dell'applicazione ... 186
Informazioni sull'aggiornamento dei database dell'applicazione ... 186
Visualizzazione delle informazioni sul database ... 187
Aggiornamento manuale ... 188
Aggiornamento pianificato ... 189
Aggiornamento in roaming ... 190
Report dell'applicazione ... 191
Informazioni sui report ... 191
Visualizzazione dei record del report ... 191

Eliminazione dei record del report ... 192
Configurazione di impostazioni aggiuntive ... 193
Modifica della password segreta ... 193
Visualizzazione dei suggerimenti ... 194
Configurazione delle notifiche acustiche ... 195
COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA ... 196
GLOSSARIO ... 197
KASPERSKY LAB ... 199
CRYPTOEX OOO ... 200
INDICE ... 201

CONTRATTO DI LICENZA CON L'UTENTE FINALE KASPERSKY LAB

AVVERTENZA LEGALE IMPORTANTE PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO PRIMA DI INIZIARE AD USARE IL SOFTWARE.

FACENDO CLIC SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O IMMETTENDO IL/I SIMBOLO/I CORRISPONDENTE/I, LEI ACCETTA DI ESSERE VINCOLATO AL RISPETTO DEI TERMINI E DELLE CONDIZIONI DI QUESTO CONTRATTO. **TALE AZIONE EQUIVALE AD APPORRE LA SUA FIRMA E SIGNIFICA CHE ACCETTA DI ESSERE VINCOLATO E DI DIVENTARE UNA PARTE CONTRAENTE DEL PRESENTE CONTRATTO E CHE ACCETTA LA VALIDITÀ LEGALE DEL PRESENTE CONTRATTO COME QUALSIASI ACCORDO STIPULATO PER ISCRITTO E DA LEI FIRMATO.** QUALORA NON SIA D'ACCORDO CON TUTTI I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO, ANNULLI L'INSTALLAZIONE DEL SOFTWARE E NON LO INSTALLI.

DOPO AVER FATTO CLIC SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O DOPO AVER IMMESSO IL/I SIMBOLO/I CORRISPONDENTE/I LEI HA DIRITTO AD UTILIZZARE IL SOFTWARE SECONDO I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO.

1. Definizioni

1.1. **Per Software** si intende il software, compresi gli aggiornamenti e i relativi materiali.

1.2. **Per Titolare** (titolare di tutti i diritti, sia esclusivi che non, relativi al Software) si intende Kaspersky Lab ZAO, una società regolarmente costituita ai sensi delle leggi della Federazione Russa.

1.3. **Per Computer** si intende l'hardware, ivi compresi i personal computer, i laptop, le postazioni di lavoro, i personal digital assistant, gli "smart phone", i dispositivi palmari o gli altri dispositivi elettronici per cui il Software è stato progettato su cui il Software verrà installato e/o utilizzato.

1.4. **Per Utente Finale (Lei/Suo)** si intende il soggetto o i soggetti che installano o utilizzano il Software per proprio conto e che sta/stanno utilizzando legalmente una copia del Software; o, se il Software è stato scaricato o installato per conto di un'organizzazione, ad esempio da un dipendente, *"Lei"* sta a intendere anche l'organizzazione per cui il Software è stato scaricato o installato e si dichiara con il presente che tale organizzazione ha autorizzato quel soggetto ad accettare questo contratto, scaricando e installando il Software per conto dell'organizzazione stessa. Ai fini del presente contratto il termine "*organizzazione"* include, a titolo esemplificativo e non limitativo, qualsiasi società di persone, società a responsabilità limitata, persona giuridica, associazione, società per azioni, trust, joint venture, organizzazione sindacale, organizzazione non registrata o autorità governativa.

1.5. **Per Partner** si intendono le organizzazioni o il soggetto/i soggetti che distribuiscono il Software al Titolare sulla base di un contratto e di una licenza.

1.6. **Per Aggiornamento/i** si intendono tutti gli aggiornamenti, le revisioni, le patch, i perfezionamenti, le correzioni, le modifiche, le copie, le aggiunte o i pacchetti di manutenzione, ecc.

1.7. **Per Manuale dell'Utente** si intende il manuale dell'utente, la guida per l'amministratore, il libro di riferimento e i relativi materiali di tipo illustrativo o di altro tipo.

2. Concessione della licenza

2.1. Con il presente il Titolare Le concede licenza di uso non esclusivo per la memorizzazione, il caricamento, l'installazione, l'esecuzione e la visualizzazione (l'"uso") del Software su di una quantità specificata di Computer al fine di fornire un supporto per la protezione del Suo Computer, sul quale è installato il Software, contro le minacce descritte nel Manuale dell'Utente, in osservanza di tutti i requisiti tecnici descritti nel Manuale dell'Utente e secondo i termini e le condizioni di questo Contratto (la "Licenza") e Lei accetta questa Licenza:
Versione di prova. Se ha ricevuto, scaricato e/o installato la versione di prova del Software e se ha aderito alla licenza di valutazione del Software, può utilizzare il Software solo a scopo dimostrativo e soltanto per il periodo dimostrativo consentito, salvo laddove diversamente indicato, a partire dalla data della prima installazione. È severamente proibito l'uso del Software per scopi diversi o per un periodo più lungo del periodo di valutazione consentito.

Software per ambiente multiplo; Software a linguaggio multiplo; Software a doppio supporto magnetico; Copie multiple; Servizi aggiuntivi. Qualora Lei utilizzi diverse versioni del Software o edizioni del Software di lingua diversa, o riceva il Software su diversi supporti magnetici, o comunque riceva copie multiple del Software, ovvero qualora in cui Lei abbia acquistato il Software insieme a software aggiuntivi, il numero massimo di Computer su cui il Software può essere installato deve corrispondere al numero di computer specificato nelle licenze ricevute dal Titolare *sempre che* ogni licenza acquisita Le dia diritto a installare e utilizzare il Software

sulla quantità numero di Computer specificata nei paragrafi 2.2 e 2.3, salvo laddove diversamente stabilito dai termini della licenza.

2.2. Se il Software è stato acquisito su un supporto fisico, Lei ha il diritto di utilizzare il Software per proteggere la quantità di Computer specificata nel pacchetto Software o secondo quanto specificato nel contratto aggiuntivo.

2.3. Se il Software è stato acquisito via Internet, Lei ha il diritto di utilizzare il Software per la protezione della quantità di Computer specificata all'atto dell'acquisizione della Licenza del Software o secondo quanto specificato nel contratto aggiuntivo.

2.4. Lei ha diritto di copiare il Software soltanto a scopo di back-up e solo a titolo di sostituzione della copia di Sua legale proprietà, qualora essa vada persa, distrutta o diventi inutilizzabile. Questa copia di back-up non può essere utilizzata per fini diversi e deve essere distrutta quando viene meno il diritto d'uso del Software o alla scadenza della Sua licenza o qualora questa venga meno per qualsiasi altro motivo, ai sensi dalla legislazione in vigore nel principale paese di residenza o nel paese in cui Lei fa uso del Software.

2.5. Dal momento in cui si procede all'attivazione del Software o dopo l'installazione del file della chiave di licenza (a eccezione della versione di prova del Software), Lei ha diritto di ricevere i seguenti servizi per il periodo di tempo specificato sul pacchetto Software (se il Software è stato acquisito su supporto fisico) o specificato durante l'acquisizione (se il Software è stato acquisito via Internet):

- Aggiornamenti del Software via Internet quando e nel momento in cui il Titolare li pubblica sul suo sito o attraverso altri servizi online. Qualsiasi Aggiornamento di cui Lei possa essere destinatario costituisce parte del Software e a esso si applicano i termini e le condizioni di questo Contratto;
- Supporto Tecnico via Internet e Hotline telefonica di Supporto Tecnico.

3. Attivazione e validità

3.1. Nel caso in cui Lei apportasse modifiche al Suo computer o al software di altri fornitori installato su di esso, il Titolare ha la facoltà di chiederLe di ripetere l'attivazione del Software o l'installazione del file della chiave di licenza. Il Titolare si riserva il diritto di utilizzare qualsiasi mezzo e qualsiasi procedura per verificare la validità della Licenza e/o la validità legale della copia del Software installata e/o utilizzata sul Suo Computer.

3.2. Se il Software è stato acquisito su supporto fisico, esso può essere utilizzato previa accettazione del presente Contratto per il periodo specificato sulla confezione a far data dalla data di accettazione del presente Contratto o secondo quanto specificato nel contratto aggiuntivo.

3.3. Se il Software è stato acquisito via Internet, il Software può essere utilizzato previa accettazione del presente Contratto per il periodo specificato durante l'acquisizione o secondo quanto specificato nel contratto aggiuntivo.

3.4. Lei ha diritto di usare la versione di prova del Software secondo quanto disposto dal Paragrafo 2.1 senza alcun addebito unicamente per il periodo di valutazione (30 giorni) concesso dal momento della sua attivazione ai sensi del presente Contratto, *purché* la versione di prova non dia diritto ad Aggiornamenti e a Supporto Tecnico via Internet e tramite Hotline telefonica. Qualora il Titolare stabilisca una durata diversa per il singolo periodo di valutazione applicabile, Lei ne sarà informato per mezzo di una notifica.

3.5. La Sua Licenza d'Uso del Software è limitata al periodo di tempo specificato nei Paragrafi 3.2 o 3.3 (secondo quanto applicabile) e nel periodo restante può essere visionata utilizzando i supporti descritti nel Manuale dell'Utente.

3.6. Nel caso in cui Lei abbia acquisito il Software per un utilizzo su più di un Computer, la Sua Licenza d'Uso del Software è limitata al periodo di tempo che ha inizio alla data di attivazione del Software o l'installazione del file della chiave di licenza sul primo Computer.

3.7. Fatto salvo qualsiasi altro rimedio previsto dalla legge o basato sui principi di opportunità, giustizia e onesta composizione ("equity") a cui il Titolare possa legittimamente fare ricorso, nel caso di una Sua violazione dei termini e delle condizioni del presente Contratto, il Titolare avrà diritto in ogni momento e senza obbligo di preavviso di rescindere questa Licenza d'uso del Software senza rimborsare il prezzo d'acquisto né parte di esso.

3.8. Lei accetta di fare uso del Software e utilizzare qualsiasi rapporto o informazione derivante dall'utilizzo di questo Software in modo conforme a tutte le leggi applicabili internazionali, nazionali, statali, regionali e locali e a qualsiasi normativa, ivi compresa, a titolo esemplificativo e non limitativo, le leggi sulla privacy, sui diritti d'autore, sul controllo delle esportazioni e sulle oscenità.

3.9. Fatte salve eventuali disposizioni contrarie specificamente previste in questa sede, Lei non ha la facoltà di trasferire né di assegnare alcuno dei diritti che le sono stati concessi ai sensi del presente Contratto né alcuno degli obblighi che da esso Le derivano.

4. Supporto Tecnico

Il Supporto Tecnico descritto al Paragrafo 2.5 del presente Contratto Le viene fornito quando è stato installato l'Aggiornamento più recente del Software (a eccezione della versione di prova del Software).
Servizio di assistenza tecnica: http://support.kaspersky.com

5. Restrizioni

5.1. Le è fatto divieto di emulare, clonare, locare, dare in prestito, noleggiare, vendere, modificare, decompilare o reingegnerizzare il Software, disassemblarlo o creare opere accessorie basate sul Software o su una porzione di esso con la sola eccezione di diritti non rinunciabili previsti dalla legislazione applicabile, e Le è fatto

comunque divieto di ridurre parte del Software in forma decifrabile o trasferire il Software tutelato da licenza o qualsivoglia sottoinsieme dello stesso, o permettere a terzi di fare quanto sopra, salvo nella misura in cui le limitazioni sopra illustrate siano espressamente proibite dal diritto applicabile. È fatto divieto di utilizzare o reingegnerizzare qualsivoglia codice binario o origine del Software allo scopo di ricreare l'algoritmo del programma, che è proprietario. Tutti i diritti non espressamente concessi attraverso il presente Contratto sono riservati al Titolare e/o ai suoi fornitori, secondo quanto applicabile. L'uso non autorizzato del Software produrrà la rescissione immediata e automatica del presente Contratto e della Licenza concessa in virtù dello stesso e può determinare l'apertura di un procedimento legale nei Suoi confronti.

5.2. Fatto salvo quanto disposto in un contratto aggiuntivo, Lei non ha diritto di trasferire i diritti d'uso del Software a terzi.

5.3. Le è fatto divieto di mettere a conoscenza di terzi il codice di attivazione e/o il file chiave della licenza o di consentire l'accesso al codice di attivazione e/o di licenza, i quali rappresentano dati riservati del Titolare; Lei sarà inoltre tenuto a usare ogni ragionevole cautela per la protezione del codice di attivazione e/o di licenza riservati, qualora Lei abbia la facoltà di trasferire il codice di attivazione e/o di licenza a terzi secondo quanto illustrato in un contratto aggiuntivo.

5.4. Non è consentito concedere a noleggio, in locazione o in prestito a terzi il Software.

5.5. Non è consentito utilizzare il Software per la creazione di dati o di software che servono a individuare, bloccare o gestire le minacce descritte nel Manuale dell'Utente.

5.6. In caso di violazione dei termini e delle condizioni del presente Contratto, il Titolare ha il diritto di bloccare il file di codice o di annullare la Sua licenza d'uso del Software senza obbligo di rimborso.

5.7. Se si usa la versione di prova del Software non si ha il diritto di ricevere il Supporto Tecnico specificato al Paragrafo 4 del presente Contratto, né il diritto di trasferire la licenza o i diritti d'uso del software a terzi

6. Garanzia limitata e clausola di esclusione della responsabilità

6.1. Il Titolare garantisce che il Software eseguirà sostanzialmente le prestazioni illustrate nelle specifiche e descritte nel Manuale dell'Utente *fermo restando, tuttavia, che* tale garanzia limitata non si applica a quanto segue: (w) lacune del Suo Computer e relative violazioni per le quali il Titolare declina espressamente qualsiasi responsabilità di garanzia; (x) malfunzionamenti, difetti o guasti conseguenti a cattivo uso, abuso, incidente, negligenza, difetti di installazione, funzionamento o manutenzione, furto, atto vandalico, evento di forza maggiore, atti di terrorismo, interruzione di tensione o momentanea sovratensione, infortunio, alterazione, modifica non consentita o riparazioni eseguite da soggetti diversi dal Titolare o qualsiasi azione o causa, a opera Sua o di qualsiasi altro soggetto terzo, ragionevolmente fuori del controllo del Titolare; (y) qualsiasi difetto da Lei tenuto nascosto al Titolare anche dopo la comparsa della prima anomalia; e (z) incompatibilità provocata da componenti hardware e/o software installati sul Suo computer.

6.2. Lei riconosce, accetta e concorda che nessun software è esente da errori e che Lei è stato informato che è necessario fare il back-up del Computer, con la frequenza e secondo le modalità per Lei più indicate.

6.3. Lei riconosce, accetta e concorda che il Titolare non è responsabile né perseguibile per l'eliminazione di dati da Lei autorizzata. I dati in questione possono includere qualsiasi informazione di natura personale o riservata.

6.4. Il Titolare non garantisce che il Software funzionerà correttamente se Lei non scarica regolarmente gli Aggiornamenti specificati nel Paragrafo 2.5 del presente Contratto.

6.5. Il Titolare non garantisce la protezione dalle minacce descritte nel Manuale dell'Utente una volta scaduto il periodo specificato nei Paragrafi 3.2 or 3.3 del presente Contratto o una volta scaduta, per qualsiasi motivo, la Licenza d'uso del Software.

6.6. IL SOFTWARE VIENE FORNITO "COSÌ COM'È" E IL TITOLARE NON FA ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA IN QUANTO A USO O PRESTAZIONI. FATTE SALVE LE GARANZIE, LE CONDIZIONI, LE DICHIARAZIONI O I TERMINI CHE NON POSSONO ESSERE ESCLUSI O LIMITATI DAL DIRITTO APPLICABILE, IL TITOLARE E I SUOI PARTNER, NON FORNISCONO ALCUNA GARANZIA, CONDIZIONE, DICHIARAZIONE O TERMINE (NÉ ESPLICITO NÉ IMPLICITO NÉ PREVISTO DALLA LEGGE, DALLA *COMMON LAW*, DALLE CONSUETUDINI O DAGLI USI O ALTRO) IN MERITO A QUALSIVOGLIA QUESTIONE, IVI COMPRESE, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, LA NON VIOLAZIONE DEI DIRITTI DI TERZI, LA COMMERCIABILITÀ, LA QUALITÀ SODDISFACENTE, L'INTEGRAZIONE O L'APPLICABILITÀ PER UN FINE SPECIFICO. LEI SI ASSUME LA RESPONSABILITÀ DI TUTTI GLI ERRORI E TUTTI I RISCHI RELATIVI ALLE PRESTAZIONI NONCHÉ LA RESPONSABILITÀ DI AVER SCELTO IL SOFTWARE ALLO SCOPO DI RAGGIUNGERE I RISULTATI DESIDERATI NONCHÉ DELL'INSTALLAZIONE DEL SOFTWARE, DEL RELATIVO USO E DEI RISULTATI OTTENUTI DALLO STESSO. SENZA LIMITARE LE DISPOSIZIONI DI CUI SOPRA, IL TITOLARE NON FORNISCE ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA CHE IL SOFTWARE SARÀ ESENTE DA ERRORI O ESENTE DA INTERRUZIONI O ALTRI DIFETTI DI FUNZIONAMENTO NÉ CHE IL SOFTWARE SARÀ IN GRADO DI SODDISFARE IN TOTO O IN PARTE LE SUE ESIGENZE, SIANO ESSE STATE COMUNICATE AL TITOLARE O MENO.

7. Esclusione e limite della responsabilità

NELLA MASSIMA MISURA CONSENTITA DAL DIRITTO APPLICABILE, IN NESSUN CASO IL TITOLARE O I SUOI PARTNER SARANNO RESPONSABILI DI DANNI SPECIALI, MARGINALI, PUNITIVI, INDIRETTI O DI DANNI INDIRETTI DI QUALSIASI TIPO (IVI COMPRESI, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, I DANNI PER

PERDITA DI UTILI O PER PERDITA DI INFORMAZIONI RISERVATE O DI ALTRE INFORMAZIONI, PER INTERRUZIONE DELL'ATTIVITÀ LAVORATIVA, PER PERDITA DI PRIVACY, PER CORRUZIONE, DANNO E PERDITA DI DATI O DI PROGRAMMI, PER MANCATA OSSERVANZA DI UN OBBLIGO IVI COMPRESO QUALSIASI ONERE IMPOSTO PER LEGGE, DOVERE DI BUONA FEDE O DOVERE DI RAGIONEVOLE DILIGENZA, PER NEGLIGENZA, PER PERDITA ECONOMICA E PER QUALSIASI ALTRA PERDITA PECUNIARIA O ALTRA PERDITA DI SORTA) DERIVANTE DA O IN QUALSIASI MODO COLLEGATO ALL'USO O ALL'IMPOSSIBILITÀ DI USARE IL SOFTWARE, ALLA FORNITURA O MANCATA FORNITURA DEL SERVIZIO DI SUPPORTO O DI ALTRI SERVIZI, INFORMAZIONI, SOFTWARE E RELATIVI CONTENUTI ATTRAVERSO IL SOFTWARE O COMUNQUE DERIVANTI DALL'USO DEL SOFTWARE O COMUNQUE AI SENSI O IN RELAZIONE A QUALSIASI DISPOSIZIONE DEL PRESENTE CONTRATTO, O DERIVANTI DA UNA VIOLAZIONE DEL PRESENTE CONTRATTO O DA QUALSIVOGLIA ILLECITO (IVI COMPRESA LA NEGLIGENZA, LA FALSA TESTIMONIANZA, QUALSIASI OBBLIGO O DOVERE RELATIVI ALLA RESPONSABILITÀ) O DA UNA VIOLAZIONE DI UN OBBLIGO DI LEGGE O DA UNA VIOLAZIONE DELLA GARANZIA DA PARTE DEL TITOLARE O DI UNO DEI SUOI PARTNER, ANCHE QUALORA IL TITOLARE O UNO DEI SUOI PARTNER SIA STATO INFORMATO DELLA POSSIBILITÀ DI TALI DANNI.

LEI ACCETTA CHE NEL CASO IN CUI IL TITOLARE E/O SUOI PARTNER VENISSERO TROVATI RESPONSABILI, LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER SI LIMITERÀ AL COSTO DEL SOFTWARE. IN NESSUN CASO LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER POTRÀ SUPERARE LE SOMME VERSATE PER IL SOFTWARE AL TITOLARE O AL PARTNER (SECONDO QUANTO APPLICABILE).

NULLA IN QUESTO CONTRATTO ESCLUDE O LIMITA LA QUALSIVOGLIA RICHIESTA DI DANNI IN CASO DI MORTE E LESIONI PERSONALI. INOLTRE IN CASO IN CUI UNA MANLEVA, ESCLUSIONE O LIMITAZIONE CONTEMPLATE DAL PRESENTE CONTRATTO NON POSSA ESSERE ESCLUSA O LIMITATA AI SENSI DEL DIRITTO APPLICABILE, QUELLA MANLEVA, ESCLUSIONE O LIMITAZIONE NON SARÀ VALIDA NEI SUOI CONFRONTI E LEI DOVRÀ CONTINUARE A OSSERVARE TUTTE LE RESTANTI MANLEVE, ESCLUSIONI E LIMITAZIONI.

8. GNU e altre licenze di Terzi

Il Software può comprendere alcuni programmi software sottoposti a licenza (o a sublicenza) dell'utente ai sensi della GNU Licenza Pubblica Generica (General Public License, GPL) o ad altra licenza software di analoga natura che, tra gli altri, concede all'utente il diritto di copiare, modificare e ridistribuire certi programmi o porzioni di essi e di avere accesso al codice source ("Software Open Source"). Se tali licenze prevedono che per un software distribuito in formato binario eseguibile anche il codice source venga reso disponibile ai suoi utenti, il codice source deve essere reso accessibile inviando la richiesta all'indirizzo source@kaspersky.com, altrimenti il codice source verrà fornito insieme al Software. Se le licenze dei Software Open Source prevedono che il Titolare fornisca diritti d'uso, di copia e modifica del programma Software Open Source più ampi dei diritti concessi in virtù del presente Contratto, tali diritti avranno la priorità sui diritti e sulle restrizioni contemplati da questo documento.

9. Proprietà Intellettuale

9.1 Lei accetta che il Software e il fatto di esserne autori, i sistemi, le idee e i metodi operativi, la documentazione e altre informazioni contenute nel Software, sono proprietà intellettuale esclusiva e/o preziosi segreti commerciali del Titolare o dei suoi partner e che il Titolare e i suoi partner, secondo quanto applicabile, sono protetti dal diritto civile e penale e dalla legge sul copyright, sul segreto commerciale, sul marchio di fabbrica e sui brevetti della Federazione Russa, dell'Unione Europea e degli Stati Uniti e da altri trattati internazionali o di altri paesi. Il presente Contratto non Le concede alcun diritto di proprietà intellettuale né alcun diritto sui marchi o sui marchi di servizio del Titolare e/o dei suoi partner ("Marchi di fabbrica"). Lei ha la facoltà di usare i marchi di fabbrica solo nella misura in cui essi permettono di identificare le stampe prodotte dal Software in conformità con la pratica sui marchi generalmente accettata, ivi compresa l'identificazione del nome del proprietario del Marchio di fabbrica. Tale uso di un Marchio di fabbrica non Le conferisce alcun diritto di proprietà sul Marchio stesso. Il Titolare e/o i relativi partner possiedono e conservano ogni diritto, titolo e interesse relativo e collegato al Software, ivi comprese, senza alcuna limitazione, le correzioni d'errore, i perfezionamenti, gli Aggiornamenti o altre modifiche del Software, sia apportate dal Titolare che da Terzi nonché tutti i diritti d'autore, i brevetti, i diritti su segreti commerciali, i marchi di fabbrica e qualsiasi altro diritto di proprietà intellettuale ivi contemplato. Il possesso, l'installazione o l'uso del Software da parte Sua non Le trasferisce alcun titolo nella proprietà intellettuale del Software e Lei non acquisirà alcun diritto sul Software, salvo nella misura espressamente indicata nel presente Contratto. Tutte le copie del Software eseguite ai sensi del presente documento devono contenere le stesse avvertenze proprietarie che compaiono sul e nel Software. Fatto salvo quanto disposto in questo documento, il presente Contratto non Le conferisce alcun diritto di proprietà intellettuale sul Software e Lei riconosce che la Licenza, secondo la definizione data in seguito, concessa ai sensi del presente Contratto Le conferisce soltanto il diritto di uso limitato ai termini e alle condizioni del presente Contratto. Il Titolare si riserva tutti i diritti che non Le sono espressamente concessi ai sensi del presente Contratto.

9.2 Lei riconosce che il codice source, il codice di attivazione e/o il file di codice di licenza per il Software sono proprietari del Titolare e che essi costituiscono segreto commerciale del Titolare. Lei accetta di non modificare, adattare, reingegnerizzare, decompilare, disassemblare, né comunque tentare di scoprire il codice source del Software.

9.3 Lei accetta di non modificare, né alterare in alcun modo il Software. Lei non ha la facoltà di rimuovere, né di alterare alcuna delle avvertenze in materia di diritti d'autore o altre avvertenze proprietarie sulle copie del Software.

10. Diritto applicabile; Arbitrato

Il presente Contratto sarà regolamentato dalle leggi della Federazione Russa e interpretato conformemente a esse, senza riferimento a conflitti fra stato di diritto e principi. Il presente Contratto non sarà regolamentato dalla Convenzione delle Nazioni Unite sui Contratti per la Vendita Internazionale di Merci, la cui applicazione è espressamente esclusa. Qualsiasi vertenza derivante dall'interpretazione o dall'applicazione dei termini del presente Contratto o dalla sua violazione dovrà essere regolata tramite trattativa diretta oppure dal Tribunale dell'Arbitrato Commerciale Internazionale avente sede presso la Camera di Commercio e dell'Industria della Federazione Russa di Mosca, Federazione Russa. Qualsiasi lodo arbitrale emesso dall'arbitro sarà definitivo e vincolante per le parti e qualsiasi giudizio su tale lodo può essere fatto valere in ogni foro competente. Nulla nel presente Paragrafo 10 può impedire a una delle Parti di ricercare e ottenere equo indennizzo presso un foro competente, sia prima, durante sia dopo il processo d'arbitrato.

11. Periodo di validità per la presentazione di azioni legali

A prescindere dalla forma, nessuna azione derivante dalle transazioni commerciali eseguite ai sensi del presente Contratto può essere presentata dalle due parti contrattuali a più di un (1) anno dal momento in cui è accaduto o si è scoperto che è accaduto l'evento su cui si basa l'azione, tranne in caso di azioni per violazione dei diritti di proprietà intellettuale, che possono essere presentate entro il periodo massimo applicabile secondo i termini di legge.

12. Totalità del Contratto; Clausola salvatoria; Assenza di deroga

Il presente Contratto costituisce l'intero contratto tra Lei e il Titolare e sostituisce ogni altro accordo, proposta, comunicato o comunicato commerciale precedente, sia verbale che scritto, relativo al Software o relativo al presente Contratto. Lei riconosce di aver letto il presente Contratto, lo comprende e accetta di essere vincolato ai suoi termini e condizioni. Se un foro competente giudica una qualsiasi disposizione del presente Contratto non valida, nulla o per qualsiasi motivo non applicabile, *in toto* o in parte, tale disposizione sarà riformulata più precisamente per renderla legittima e applicabile; ciò tuttavia non inficerà il Contratto e le rimanenti disposizioni del Contratto resteranno pienamente valide e in vigore nella massima misura consentita dalla legge diritto o dall'equity, conservando quanto più possibile il loro intento originale. Non varrà alcuna deroga a disposizioni o a condizioni del presente Contratto, a meno che la deroga non sia presentata per iscritto e firmata da Lei e da rappresentante autorizzato del Titolare, purché nessuna deroga a una violazione di una disposizione del presente Contratto valga come una deroga a qualsiasi violazione precedente, concorrente o successiva. La mancata insistenza da parte del Titolare nel richiedere la stretta applicazione di qualsiasi disposizione del presente Contratto o nel far valere un diritto non potrà essere interpretata quale deroga a tale disposizione o rinuncia a tale diritto.

13. Informazioni di contatto del Titolare

Per qualsiasi domanda relativa al presente Contratto, o se si desidera consultare per qualsiasi motivo il Titolare, si prega di contattare il nostro Servizio Clienti presso:

Kaspersky Lab ZAO, 10 edificio 1 1st Volokolamsky Proezd
Mosca, 123060
Federazione Russa
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Sito Web: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Tutti i diritti riservati. Il Software e la documentazione d'accompagnamento sono soggetti a diritto d'autore e sono protetti dalle leggi sul copyright e dai trattati internazionali sul copyright nonché da altre leggi e trattati in materia di proprietà intellettuale.

KASPERSKY MOBILE SECURITY 9.0

Kaspersky Mobile Security 9.0 assicura la protezione dei dispositivi mobili con sistema operativo Symbian e Microsoft Windows Mobile da minacce note e nuove, da chiamate e messaggi SMS indesiderati. L'applicazione consente di gestire i messaggi SMS in uscita, l'attività di rete e protegge le informazioni riservate dall'accesso non autorizzato. Ogni tipo di minaccia viene elaborato da componenti distinti del programma. Ciò consente di ottimizzare le impostazioni dell'applicazione in base alle esigenze dell'utente.

Kaspersky Mobile Security 9.0 comprende i seguenti componenti di protezione:

- **Protezione**. Protegge il file system del dispositivo mobile da infezioni. Il componente Protezione viene avviato all'avvio del sistema operativo, rimane sempre attivo nella memoria operativa del dispositivo e verifica tutti i file aperti, salvati e avviati sul dispositivo, incluse le schede di memoria. Inoltre, il componente Protezione verifica tutti i file in entrata per individuare l'esistenza di virus noti. È possibile continuare a lavorare con il file se l'oggetto non è infetto o se è stato disinfettato correttamente.

- **Scansione del dispositivo**. Facilita l'individuazione e la neutralizzazione di eventuali oggetti nocivi presenti nel dispositivo. Si consiglia di eseguire la scansione del dispositivo regolarmente per evitare la diffusione di oggetti nocivi non rilevati dalla Protezione.

- **Anti-Spam**. Verifica tutti i messaggi SMS e le chiamate in entrata per rilevare se si tratta di spam. Il componente consente di bloccare tutti i messaggi SMS e le chiamate considerati come indesiderati.

- **Parental Control**. Controlla i messaggi in uscita e impedisce l'invio di messaggi SMS e/o l'esecuzione di chiamate ai numeri di abbonati precedentemente specificati.

- **Antifurto**. Protegge le informazioni presenti sul dispositivo dall'accesso non autorizzato in caso di smarrimento o furto. Questo componente consente di bloccare il dispositivo in caso di furto o smarrimento, cancellare le informazioni riservate, controllare l'utilizzo della scheda SIM e determinare le coordinate geografiche del dispositivo (se il dispositivo mobile è dotato di un ricevitore GPS).

- **Protezione privacy**. Le informazioni riservate dell'utente sono nascoste quando il dispositivo viene utilizzato da altre persone. Il componente consente di visualizzare o nascondere tutte le informazioni relative ai numeri degli abbonati specificati, ad esempio i dettagli nell'Elenco contatti, i messaggi SMS o le voci nel registro chiamate. Il componente consente di nascondere il recapito delle chiamate e dei messaggi SMS in entrata da numeri preferiti.

- **Firewall**. Controlla le connessioni di rete sul dispositivo mobile. Il componente consente di impostare le connessioni consentite o bloccate.

- **Criptaggio**. Protegge le informazioni dalla visualizzazione di terze persone anche in caso queste riescano ad avere accesso al dispositivo. Il componente consente di criptare qualsiasi numero di cartelle non di sistema presenti nella memoria del dispositivo o su una scheda di memoria. I dati presenti nella cartella diventano disponibili solo dopo l'immissione della password segreta.

Inoltre, l'applicazione contiene una serie di funzioni di servizio sviluppate per tenere aggiornata l'applicazione, migliorarne le prestazioni e assistere gli utenti.

- Aggiornamento dei database dell'applicazione. Questa funzione mantiene aggiornati i database di Kaspersky Mobile Security 9.0.

- Stato di protezione. Sullo schermo viene visualizzato lo stato dei componenti del programma. In base alle informazioni presentate, è possibile valutare lo stato corrente della protezione sul dispositivo.

- Report eventi. Ognuno dei componenti dell'applicazione dispone del proprio report eventi che include informazioni sul funzionamento del componente (ad esempio, operazione completata, dati su un oggetto bloccato, report di scansione, aggiornamenti, ecc.).

- Licenza. Quando si acquista Kaspersky Mobile Security 9.0, tra l'utente e Kaspersky Lab intercorre un contratto di licenza, in base al quale l'utente può utilizzare l'applicazione e accedere agli aggiornamenti dei database

dell'applicazione e al Servizio di assistenza tecnica entro un determinato periodo di tempo. I termini di utilizzo e le altre informazioni necessarie per l'uso di tutte le funzioni dell'applicazione sono indicate nella licenza.

Utilizzando l'opzione **Licenza**, è possibile ottenere un report dettagliato sulla licenza corrente nonché rinnovarla.

Kaspersky Mobile Security 9.0 non supporta le operazioni di backup e ripristino.

IN QUESTA SEZIONE

Come ottenere informazioni sull'applicazione 14

Novità di Kaspersky Mobile Security 9.0 15

Requisiti Hardware e Software 16

Kit di distribuzione 16

COME OTTENERE INFORMAZIONI SULL'APPLICAZIONE

Sono sempre disponibili risposte ad ogni eventuali domanda sull'acquisto, sull'installazione o sull'utilizzo di Kaspersky Mobile Security.

Kaspersky Lab offre varie fonti di informazione sull'applicazione, tra le quali l'utente può scegliere quella più adatta all'importanza e all'urgenza della domanda.

IN QUESTA SEZIONE

Fonti di informazione per ulteriori ricerche 14

Come contattare l'Ufficio Vendite 15

Forum Web di discussione sulle applicazioni Kaspersky Lab 15

FONTI DI INFORMAZIONE PER ULTERIORI RICERCHE

Sono disponibili le seguenti fonti di informazione sull'applicazione:

- sito Web dedicato all'applicazione Kaspersky Lab;
- pagine di Knowledge Base dell'applicazione sul sito Web del Servizio di assistenza tecnica;
- guida in linea e suggerimenti installati;
- documentazione dell'applicazione installata.

Pagine dedicate all'applicazione sul sito Web di Kaspersky Lab

http://www.kasperskystore.it/cata_home.html

Consultare queste pagine per ottenere informazioni di carattere generale sulle funzioni e opzioni di Kaspersky Mobile Security. Presso il nostro E-Store è possibile acquistare Kaspersky Mobile Security.

Pagine dedicate all'applicazione sul sito Web del Servizio di assistenza tecnica (Knowledge Base).

http://www.kaspersky.com/it/service

Queste pagine contengono articoli scritti dagli esperti del Servizio di assistenza tecnica.

Questi articoli contengono informazioni utili, consigli e risposte alle domande più frequenti (FAQ) relative all'acquisto, installazione e utilizzo di Kaspersky Mobile Security. Essi sono organizzati per argomento, ad esempio "Utilizzo dei file chiave", "Aggiornamenti del database" e "Risoluzione dei problemi". Lo scopo di questi articoli è di rispondere a domande su Kaspersky Mobile Security nonché su altri prodotti Kaspersky Lab. Essi possono contenere inoltre notizie dal Servizio di assistenza tecnica.

Guida in linea installata

Il pacchetto di installazione dell'applicazione comprende file della guida completa e della guida rapida sensibile al contesto.

Per visualizzare la guida rapida, aprire la scheda corrispondente e selezionare **Guida**.

Documentazione installata

La Guida dell'Utente contiene informazioni dettagliate sulle funzioni dell'applicazione e sul loro utilizzo, insieme a suggerimenti e raccomandazioni sulla configurazione dell'applicazione.

I documenti sono inclusi in formato PDF nel pacchetto di distribuzione di Kaspersky Mobile Security.

È possibile anche scaricare questi documenti in formato elettronico dal sito Web di Kaspersky Lab.

COME CONTATTARE L'UFFICIO VENDITE

Per eventuali domande sulla selezione or sull'acquisto di Kaspersky Mobile Security o per estendere la licenza, è possibile contattare telefonicamente i nostri esperti dell'Ufficio Vendite presso la Sede Centrale di Mosca ai seguenti numeri telefonici:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

Il servizio è offerto in inglese o russo.

È possibile anche inviare le proprie domande all'Uffici Vendite via e-mail all'indirizzo sales@kaspersky.com.

FORUM WEB DI DISCUSSIONE SULLE APPLICAZIONI KASPERSKY LAB

Per domande di natura non urgente, è possibile rivolgersi agli esperti di Kaspersky Lab e mettersi in contatto con altri utenti delle applicazioni anti-virus Kaspersky Lab nel nostro forum all'indirizzo http://forum.kaspersky.com.

Nel forum è possibile visualizzare le discussioni in corso, lasciare i propri commenti, creare nuovi argomenti di discussione o utilizzare il motore di ricerca per domande specifiche.

NOVITÀ DI KASPERSKY MOBILE SECURITY 9.0

Di seguito è riportata una descrizione dettagliata delle novità introdotte da Kaspersky Mobile Security 9.0.

Nuova protezione:

- L'accesso all'applicazione è protetto da una password segreta.

- Il pacchetto di Kaspersky Mobile Security 9.0 comprende il componente Protezione privacy, che impedisce l'accesso non autorizzato ai dati personali dell'utente durante l'uso temporaneo da parte di persone non autorizzate. Il componente nasconde gli eventi dei dati ad un elenco di numeri specificato. Protezione privacy non rivela in nessun modo la sua attività, ossia non vi è alcuna indicazione dell'esistenza di dati nascosti sul dispositivo.

- Nel componente Criptaggio aggiornato è stato implementato il blocco dell'accesso a qualsiasi numero di file salvati nella memoria del dispositivo o su una scheda di memoria. Il componente protegge i dati riservati in modalità criptata e blocca automaticamente l'accesso allo scadere di un periodo di tempo specificato.

- È stato implementato un nuovo approccio alla gestione della protezione del dispositivo: l'utente può abilitare e disabilitare qualunque componente in base alla funzionalità richiesta.

- È possibile ora acquistare un codice di attivazione e rinnovare la licenza online direttamente dal dispositivo mobile.

REQUISITI HARDWARE E SOFTWARE

Kaspersky Mobile Security 9.0 è stato sviluppato per essere installato su dispositivi mobili basati su uno dei seguenti sistemi operativi:

- Sistema operativo Symbian 9.1, 9.2, 9.3 e 9.4 IU Serie 60.

- Microsoft Windows Mobile 5.0, 6.0, 6.1 o 6.5.

KIT DI DISTRIBUZIONE

È possibile acquistare Kaspersky Mobile Security online; in questo caso, il kit di distribuzione e dell'applicazione e la relativa documentazione vengono forniti in formato elettronico. Kaspersky Mobile Security può essere acquistato anche presso tutti i migliori negozi di telefonia e apparecchi tecnologici. Per informazioni dettagliate sull'acquisto dell'applicazione e sulla ricezione del kit di distribuzione, contattare il nostro Ufficio Vendite all'indirizzo sales@kaspersky.com.

KASPERSKY MOBILE SECURITY 9.0 PER SISTEMA OPERATIVO SYMBIAN

Questa sezione descrive il funzionamento di Kaspersky Mobile Security 9.0 per dispositivi mobili con sistema operativo Symbian versione 9.1, 9.2, 9.3 e 9.4 IU Serie 60.

IN QUESTA SEZIONE

Installazione di Kaspersky Mobile Security 9.0 17

Disinstallazione dell'applicazione 18

Aggiornamento dell'applicazione dalla versione 8.0 alla versione 9.0 21

Operazioni preliminari 22

Gestione della licenza 28

Interfaccia dell'applicazione 33

Protezione del file system 36

Scansione del dispositivo 40

Quarantena degli oggetti potenzialmente infetti 48

Filtro delle chiamate e dei messaggi SMS in entrata 50

Limitazione delle chiamate e dei messaggi SMS in uscita. Parental Control 63

Protezione dei dati in caso di smarrimento o furto del dispositivo 71

Mascheramento dei dati personali 81

Filtro dell'attività di rete. Firewall 89

Criptaggio 92

Aggiornamento dei database dell'applicazione 96

Report dell'applicazione 102

Configurazione di impostazioni aggiuntive 104

INSTALLAZIONE DI KASPERSKY MOBILE SECURITY 9.0

L'installazione dell'applicazione su un dispositivo mobile viene eseguita mediante alcuni passaggi.

Per installare Kaspersky Mobile Security 9.0:

1. Collegare il dispositivo mobile al computer.

   Per i dispositivi mobili Nokia, si consiglia di utilizzare l'applicazione Nokia PC Suite.

2. Eseguire una delle seguenti operazioni:

   - Se si è acquistato il programma su CD, eseguire l'installazione automatica di Kaspersky Mobile Security 9.0 dal CD acquistato.
   - Se si è acquistato il pacchetto di distribuzione su Internet, copiarlo sul dispositivo mobile utilizzando uno dei seguenti metodi:
     - utilizzando l'applicazione Nokia PC Suite (per dispositivi mobili Nokia);
     - utilizzando una scheda di memoria.

     Avviare l'installazione utilizzando uno dei seguenti metodi:

     - dall'applicazione Nokia PC Suite (per dispositivi mobili Nokia);
     - aprire l'archivio sis contenente il pacchetto di distribuzione sul dispositivo mobile.

   Verrà visualizzata una finestra di conferma dell'installazione.

3. Confermare l'installazione dell'applicazione premendo il pulsante **Sì**.

4. Esaminare le informazioni aggiuntive sull'applicazione, comprendenti nome, versione e certificati. Quindi premere **Continua**.

   Se la lingua del sistema operativo non corrisponde alla lingua di Kaspersky Mobile Security 9.0, sullo schermo verrà visualizzato un messaggio. Per procedere con l'installazione nella lingua corrente, premere **OK**.

5. Leggere il testo del Contratto di licenza che intercorre tra l'utente e Kaspersky Lab. Per accettare tutti i termini del contratto, premere **OK**. Kaspersky Mobile Security 9.0 verrà installato sul dispositivo. Se non si accettano i termini del Contratto di licenza, premere **Annulla**. In questo modo, l'installazione verrà interrotta.

6. Verificare che sul dispositivo non siano presenti altre applicazioni anti-virus premendo **OK**.

7. Riavviare il dispositivo per completare l'installazione.

   L'applicazione viene installata con i parametri consigliati dagli esperti di Kaspersky Lab.

DISINSTALLAZIONE DELL'APPLICAZIONE

Per disinstallare Kaspersky Mobile Security 9.0:

1. Decriptare i dati sul dispositivo se questi sono stati criptati con Kaspersky Mobile Security 9.0 (vedere la sezione "Decriptaggio dei dati" a pagina 94).

2. Disabilitare Protezione privacy (vedere la sezione "Modi Protezione privacy" a pagina 82).

3. Chiudere Kaspersky Mobile Security 9.0 selezionando **Opzioni** → **Esci** (vedere la figura sotto).

Figura 1. Uscita dall'applicazione

4. Disinstallare di Kaspersky Mobile Security 9.0 eseguendo le seguenti operazioni:

   a. Aprire il menu principale del dispositivo.

   b. Selezionare la cartella **Applicazioni** → **Gest. applic.** → **Applic. installate** (vedere la figura sotto).

La cartella di installazione dell'applicazione può variare a seconda del modello del dispositivo mobile.

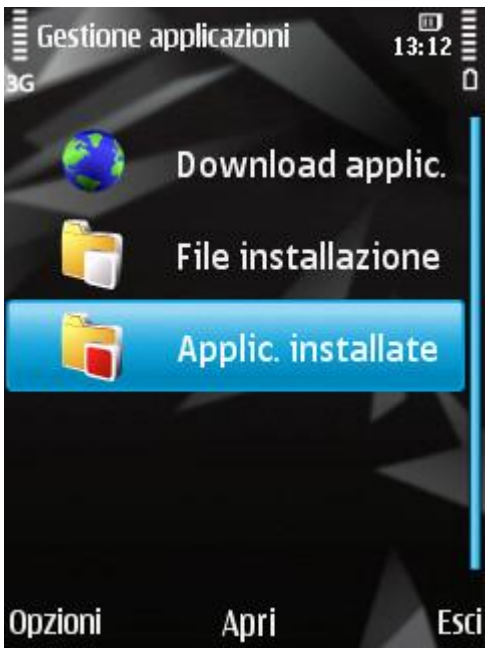


Figura 2. Avvio di Gestione applicazioni

c. Selezionare **KMS 9.0** dall'elenco delle applicazioni, quindi selezionare **Opzioni** → **Disinstalla** (vedere la figura sotto).

Figura 3. Rimozione dell'applicazione

d. Confermare la disinstallazione dell'applicazione premendo il pulsante **Sì**.

e. Immettere la password segreta e premere **OK**.

f. Specificare se conservare o meno le impostazioni del programma e gli oggetti in quarantena:

- Se si desidera salvare i parametri dell'applicazione e gli oggetti in quarantena, selezionare le caselle accanto ai parametri richiesti e premere **OK** (vedere la figura sotto).

- Per disinstallare completamente l'applicazione, premere **Annulla**.

Figura 4. Elenco delle impostazioni da salvare

5. Riavviare il dispositivo per completare la disinstallazione dell'applicazione.

AGGIORNAMENTO DELL'APPLICAZIONE DALLA VERSIONE 8.0 ALLA VERSIONE 9.0

Se sul dispositivo mobile è già installato Kaspersky Mobile Security 8.0, è possibile aggiornarlo alla versione 9.0.

Prima di aggiornare la versione dell'applicazione, disabilitare Criptaggio – decripta tutti i dati (vedere la sezione "Decriptaggio dei dati" a pagina 94).

Per aggiornare la versione del programma:

1. Chiudere la versione corrente di Kaspersky Mobile Security premendo **Opzioni** → **Esci**.
2. Copiare il pacchetto di distribuzione dell'applicazione sul dispositivo utilizzando uno dei seguenti metodi:
   - dal sito Web di Kaspersky Lab;
   - utilizzando l'applicazione Nokia PC Suite (per dispositivi mobili Nokia);
   - utilizzando una scheda di memoria.
3. Avviare il pacchetto di distribuzione di Kaspersky Mobile Security 9.0 sul dispositivo.
4. Confermare l'installazione dell'applicazione premendo il pulsante **Sì**.
5. Esaminare le informazioni aggiuntive sull'applicazione, comprendenti nome, versione e certificati. Quindi premere **Continua**.
6. Confermare l'aggiornamento della versione dell'applicazione premendo **OK**.

7. Immettere la password segreta impostata nella versione precedente dell'applicazione.

8. Leggere attentamente il contratto di licenza. Per accettare i termini del contratto, premere **OK**. Se non si accettano i termini del Contratto di licenza, premere **Annulla**. In questo modo, l'installazione verrà interrotta.

9. Verificare che sul dispositivo non siano presenti altre applicazioni anti-virus premendo **OK**.

10. Eliminare le impostazioni configurate della versione precedente dell'applicazione premendo **Elimina**.

    Le impostazioni possono essere salvate durante il passaggio da una versione all'altra nell'ambito della stessa generazione di prodotti. I parametri della versione 8.0 dell'applicazione non sono compatibili con la versione 9.0.

    Verrà avviata l'installazione di Kaspersky Mobile Security 9.0.

    Se il periodo di validità della licenza di Kaspersky Mobile Security 8.0 non è scaduto, abilitare la versione 9.0 del programma utilizzando il codice di attivazione della versione 8.0 (vedere la sezione "Attivazione dell'applicazione" a pagina 22).

11. Riavviare il dispositivo per completare l'installazione.

OPERAZIONI PRELIMINARI

Questa sezione contiene informazioni su come preparare Kaspersky Mobile Security 9.0 per il funzionamento (attivazione e creazione di una password segreta), eseguire l'applicazione, aggiornare i suoi database ed eseguire la scansione anti-virus del dispositivo.

IN QUESTA SEZIONE

Attivazione dell'applicazione....22

Immissione della password segreta....26

Avvio dell'applicazione....27

Aggiornamento dei database dell'applicazione....27

Scansione anti-virus del dispositivo....28

Visualizzazione di informazioni sull'applicazione....28

ATTIVAZIONE DELL'APPLICAZIONE

Per poter utilizzare Kaspersky Mobile Security 9.0, è necessario prima attivarlo. Durante il processo di attivazione, è necessario immettere un codice di attivazione che viene verificato e registrato sui server Kaspersky Lab. Successivamente, l'applicazione riceverà e installerà un file chiave.

È possibile ottenere un codice di attivazione nei seguenti modi:

- online (vedere la sezione "Acquisto di un codice di attivazione online" a pagina 25), uscendo dall'applicazione Kaspersky Mobile Security 9.0 e passando al sito Web;
- sul sito Web all'indirizzo http://www.kasperskystore.it;
- dai distributori Kaspersky Lab.

Per attivare Kaspersky Mobile Security 9.0 sul proprio dispositivo è necessario disporre di una connessione Internet configurata.

Prima di attivare l'applicazione, assicurarsi che le impostazioni della data di sistema del dispositivo siano corrette.

È possibile attivare l'applicazione nei seguenti modi:

- **Attivare la licenza trial**. Selezionare questo metodo di attivazione se si desidera acquisire dimestichezza con le funzioni dell'applicazione e acquistare la versione commerciale in un secondo momento. Durante l'attivazione verrà installato un file chiave gratuito. Al completamento dell'attivazione, sullo schermo verrà visualizzato il periodo di validità della licenza trial. Alla scadenza del periodo di validità della licenza trial, le funzioni dell'applicazione saranno limitate. Saranno disponibili solo le seguenti funzioni:
  - attivazione dell'applicazione;
  - gestione della licenza dell'applicazione;
  - guida in linea di Kaspersky Mobile Security 9.0;
  - disabilitazione del componente Criptaggio;
  - disabilitazione del componente Protezione privacy.

  Non è possibile riattivare una licenza trial.
- **Attivare la licenza commerciale**. Selezionare questo metodo se si è acquistata la versione commerciale dell'applicazione e si è ottenuto un codice di attivazione. Dopo aver immesso il codice di attivazione, verrà ricevuto e installato un file chiave che fornisce l'accesso alla gamma completa delle funzioni dell'applicazione. Sullo schermo del dispositivo verrà visualizzato il periodo di validità. Alla scadenza del periodo di validità, le funzioni dell'applicazione saranno limitate; l'applicazione non verrà più aggiornata.

IN QUESTA SEZIONE

Attivazione della versione commerciale 23

Attivazione della versione trial 24

Acquisto online di un codice di attivazione 25

ATTIVAZIONE DELLA VERSIONE COMMERCIALE

Per attivare la versione commerciale dell'applicazione con il codice di attivazione:

1. Aprire il menu principale del dispositivo.
2. Selezionare la cartella **Applicazioni** → **KMS 9.0**.

   La cartella di installazione dell'applicazione può variare a seconda del modello del dispositivo mobile.
3. Avviare l'applicazione premendo **Opzioni** → **Apri**.

   Verrà aperta la finestra **KMS 9.0**.
4. Selezionare **Opzioni** → **Immetti codice**.

   Si aprirà la finestra di attivazione di Kaspersky Mobile Security 9.0.

5. Immettere il codice nei quattro campi. Il codice di attivazione è composto da caratteri dell'alfabeto latino e cifre e non distingue tra maiuscole e minuscole. Dopo aver immesso il codice di attivazione, selezionare **Opzioni** → **Attiva** (vedere la figura sotto).

Figura 5. Attivazione di una versione commerciale dell'applicazione

6. Confermare la connessione a Internet premendo **Sì**.

7. Selezionare il punto di accesso attraverso cui verrà eseguita la connessione al server di attivazione di Kaspersky Lab.

   L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab. Dopo aver verificato il codice di attivazione, l'applicazione scaricherà e installerà il file chiave.

   Se per qualche motivo il codice di attivazione immesso non risulta valido, sullo schermo verrà visualizzato un messaggio informativo. In questo caso, si consiglia di verificare che il codice di attivazione immesso sia corretto e di contattare il rivenditore del software presso cui è stato acquistato Kaspersky Mobile Security 9.0.

   Se si sono verificati errori durante la connessione al server e non è stato possibile ottenere una chiave di licenza, l'attivazione verrà annullata. In questo caso, si consiglia di verificare i parametri di connessione a Internet. Se non è stato possibile correggere gli errori, contattare l'Assistenza tecnica.

8. Passare all'immissione della password segreta (vedere la sezione "Immissione della password segreta" a pagina 26).

ATTIVAZIONE DELLA VERSIONE TRIAL

Per attivare la licenza trial di Kaspersky Mobile Security 9.0:

1. Aprire il menu principale del dispositivo.

2. Selezionare la cartella **Applicazioni** → **KMS 9.0**.

   La cartella di installazione dell'applicazione può variare a seconda del modello del dispositivo mobile.

3. Avviare l'applicazione premendo **Opzioni** → **Apri**.

   Verrà aperta la finestra **KMS 9.0**.

4. Selezionare **Opzioni**→ **Versione trial** (vedere la figura sotto).

Figura 6. Attivazione di una versione commerciale dell'applicazione

5. Confermare la connessione a Internet premendo **Sì**.

6. Selezionare il punto di accesso attraverso cui verrà eseguita la connessione al server di attivazione di Kaspersky Lab e premere **OK**.

   L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e scaricherà e installerà il file chiave.

   Se si sono verificati errori durante la connessione al server e non è stato possibile ottenere una chiave di licenza, contattare l'Assistenza tecnica.

7. Passare all'immissione della password segreta (vedere la sezione "Immissione della password segreta" a pagina 26).

ACQUISTO ONLINE DI UN CODICE DI ATTIVAZIONE

Per acquistare online un codice di attivazione per l'applicazione, eseguire le seguenti operazioni:

1. Aprire il menu principale del dispositivo.

2. Selezionare la cartella **Applicazioni** → **KMS 9.0**.

   La cartella di installazione dell'applicazione può variare a seconda del modello del dispositivo mobile.

3. Avviare l'applicazione premendo **Opzioni** → **Apri**.

   Verrà aperta la finestra **KMS 9.0**.

4. Selezionare **Opzioni** → **Acquista online**.

   Verrà aperta la finestra **Acquista online**.

5. Premere **Apri** (vedere la figura sotto).

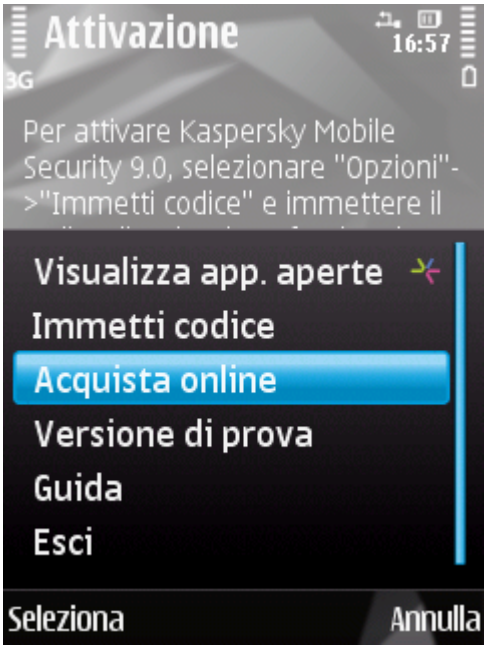


Figura 7. Acquisto online del codice di attivazione

Verrà aperto il sito Web in cui verrà chiesto di effettuare un ordine per l'acquisto online del codice di attivazione.

6. Seguire le istruzioni dettagliate.

7. Al termine dell'acquisto del codice di attivazione, passare all'attivazione della versione commerciale dell'applicazione (vedere la sezione "Attivazione della versione commerciale" a pagina 23).

IMMISSIONE DELLA PASSWORD SEGRETA

Al termine dell'attivazione del programma, verrà chiesto di immettere la password segreta. La *password segreta* impedisce l'accesso non autorizzato alle impostazioni dell'applicazione. È possibile cambiare in un secondo momento la password segreta installata.

La password segreta viene richiesta nei seguenti casi:

- per l'accesso all'applicazione;
- per l'accesso ai dati criptati;
- per abilitare/disabilitare il componente Protezione privacy;
- quando si invia un comando con uno speciale messaggio SMS per avviare le seguenti funzioni in remoto: SMS-Block, SMS-Clean, SIM Watch, SMS-Find, Protezione privacy;
- in caso di disinstallazione dell'applicazione.

Si raccomanda di non dimenticare la password segreta. Se si dimentica la password segreta, sarà impossibile utilizzare le funzioni di Kaspersky Mobile Security 9.0 oppure ottenere l'accesso ai dati criptati e disinstallare l'applicazione.

Si consiglia di scegliere una password segreta composta da almeno 7 cifre.

Per immettere la password segreta:

1. Al termine dell'attivazione dell'applicazione, immettere nel campo **Immettere nuova password** le cifre che comporranno la password.
2. Ripetere l'immissione dello stesso codice nel campo **Conferma**.

   Il codice immesso viene verificato automaticamente.
3. Se il codice viene considerato non valido in base ai risultati della verifica, verrà visualizzato un messaggio di avviso e l'applicazione richiederà una conferma. Per utilizzare il codice, premere **Sì**. Per creare una nuova password, premere **No**.
4. Per iniziare a utilizzare l'applicazione, premere **OK**.

AVVIO DELL'APPLICAZIONE

Per avviare Kaspersky Mobile Security 9.0:

1. Aprire il menu principale del dispositivo.
2. Selezionare la cartella **Applicazioni** → **KMS 9.0**.

   La cartella di installazione dell'applicazione può variare a seconda del modello del dispositivo mobile.
3. Avviare l'applicazione premendo **Opzioni** → **Apri**.

   Verrà aperta la finestra **KMS 9.0**.
4. Immettere la password segreta e premere **OK**.

L'applicazione visualizza una finestra che mostra lo stato corrente di Kaspersky Mobile Security 9.0 (vedere la sezione "Finestra Stato di protezione" a pagina 34). Per passare alle funzioni dell'applicazione, premere **OK**.

AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

Kaspersky Mobile Security 9.0 esegue la scansione delle minacce in base ai database dell'applicazione, che contengono le descrizioni di tutti i programmi dannosi noti attualmente e i metodi per neutralizzarli, nonché le descrizioni di altri oggetti indesiderati. Al momento dell'installazione dell'applicazione, i database inclusi nel pacchetto di installazione di Kaspersky Mobile Security 9.0 possono risultare obsoleti.

Si consiglia di aggiornare i database dell'applicazione immediatamente dopo l'installazione dell'applicazione.

Per aggiornare i database dell'applicazione è necessario disporre di una connessione Internet configurata sul proprio dispositivo mobile.

Per avviare manualmente il processo di aggiornamento del database:

1. Selezionare l'opzione **Aggiornamento** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Aggiornamento**.
2. Selezionare l'opzione **Aggiornamento**.

L'applicazione avvia il processo di aggiornamento dei database dal server Kaspersky Lab. Le informazioni sul processo di aggiornamento vengono visualizzate sullo schermo.

SCANSIONE ANTI-VIRUS DEL DISPOSITIVO

Al termine dell'installazione dell'applicazione, si consiglia di eseguire immediatamente una scansione del dispositivo mobile per individuare eventuali oggetti malware.

La prima scansione viene eseguita con le impostazioni predefinite dagli esperti Kaspersky Lab.

Per eseguire una scansione completa del dispositivo:

1. Selezionare l'opzione **Scansione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Scansione**.

2. Selezionare **Scansione compl.**.

VISUALIZZAZIONE DI INFORMAZIONI SULL'APPLICAZIONE

È possibile visualizzare informazioni di carattere generale sull'applicazione, comprendenti il numero di versione e dettagli sul copyright.

Per visualizzare le informazioni sull'applicazione,

nella scheda **Avanzate**, selezionare **Info**.

GESTIONE DELLA LICENZA

Nell'ambito della gestione delle licenze delle applicazioni Kaspersky Lab, è importante conoscere i seguenti tre termini:

- Contratto di licenza;
- licenza;
- file chiave.

Tali termini sono inseparabilmente interconnessi e costituiscono un unico modello di gestione della licenza.

La seguente sezione descrive con maggiore dettaglio ognuno di questi termini.

La sezione spiega inoltre come reperire informazioni sulla licenza di Kaspersky Mobile Security 9.0 e su come estendere il suo periodo di validità.

IN QUESTA SEZIONE

Informazioni sul Contratto di licenza....29

Informazioni sulle licenze di Kaspersky Mobile Security....29

Informazioni sui file chiave di Kaspersky Mobile Security....29

Visualizzazione delle informazioni sulla licenza....30

Rinnovo della licenza....31

INFORMAZIONI SUL CONTRATTO DI LICENZA

Il *Contratto di licenza* è un accordo che intercorre tra Kaspersky Lab e la persona fisica o il soggetto giuridico che detiene legalmente una copia di Kaspersky Mobile Security. Tale contratto è incluso in ogni applicazione Kaspersky Lab e contiene informazioni dettagliate sui diritti e sulle limitazioni di utilizzo di Kaspersky Mobile Security.

Secondo quanto previsto dal Contratto di licenza, al momento dell'acquisto e dell'installazione di un'applicazione Kaspersky Lab, si ottiene il diritto illimitato di possederne la copia.

Kaspersky Lab offre inoltre i seguenti servizi aggiuntivi:

- assistenza tecnica;
- aggiornamento dei database di Kaspersky Mobile Security;
- moduli di programma dell'aggiornamento di Kaspersky Mobile Security.

Per poter usufruire di questi servizi, è necessario acquistare e attivare una licenza (vedere la sezione "Informazioni sulle licenze di Kaspersky Mobile Security" a pagina 29).

INFORMAZIONI SULLE LICENZE DI KASPERSKY MOBILE SECURITY

Una *licenza* consiste nel diritto di utilizzo di Kaspersky Mobile Security e di usufruire dei servizi aggiuntivi (vedere la sezione "Informazioni sul Contratto di licenza" a pagina 29) ad esso associati così come forniti da Kaspersky Lab o dai suoi partner.

Ogni licenza ha un periodo di validità distinto.

Il *periodo di validità della licenza* consiste nel periodo durante il quale vengono forniti all'utente servizi aggiuntivi. L'ambito dei servizi forniti dipende dal tipo di licenza.

Sono disponibili i seguenti tipi di licenza:

Trial, una licenza gratuita avente un periodo di validità limitato. Tale licenza viene offerta per consentire all'utente di conoscere e valutare Kaspersky Mobile Security. Viene fornita con una versione di prova dell'applicazione e ha un periodo di validità breve durante il quale l'utente può accedere alla Knowledge Base (http://www.kaspersky.com/it/service) e al forum (http://forum.kaspersky.com/index.php?showforum=62). Durante l'utilizzo dell'applicazione con licenza trial non è possibile contattare l'assistenza tecnica e al termine del suo periodo di validità non saranno più disponibili tutte le funzioni di Kaspersky Mobile Security.

Commerciale , una licenza a pagamento avente un periodo di validità normalmente non inferiore a un anno. Tale licenza viene concessa all'utente al momento dell'acquisto dell'applicazione. Al termine del periodo di validità della licenza commerciale di Kaspersky Mobile Security, alcune funzioni dell'applicazione diventeranno inaccessibili e i database dell'applicazione non verranno più aggiornati. In questo caso, la protezione completa del dispositivo non può essere garantita.

Per poter utilizzare l'applicazione e usufruire dei servizi aggiuntivi è necessario acquistare e attivare una licenza commerciale.

La licenza viene attivata installando il file chiave (vedere la sezione "Informazioni sui file chiave di Kaspersky Mobile Security" a pagina 29) collegato alla licenza.

INFORMAZIONI SUI FILE CHIAVE DI KASPERSKY MOBILE SECURITY

Il *file chiave* è un file che funge da chiave personale necessaria per l'utilizzo dell'applicazione. Il file chiave è un componente tecnologico che consente di attivare una licenza collegata ad esso e costituisce inoltre il diritto dell'utente di utilizzo dell'applicazione e dei servizi aggiuntivi.

Il file chiave è incluso nel kit di distribuzione dell'applicazione, se questa viene acquistata presso un rivenditore Kaspersky Lab, oppure viene inviato all'utente via e-mail, se l'applicazione viene acquistata sul negozio su Internet.

Il file chiave comprende le seguenti informazioni:

- Periodo di validità della licenza.
- Tipo di licenza (trial, commerciale).
- Limitazioni della licenza (ad esempio, numero di computer su cui la licenza è valida o volume del traffico e-mail protetto).
- Contatti di assistenza tecnica.
- Periodo di validità del file chiave.

Il *periodo di validità del file chiave*, ossia la data di scadenza associata al file chiave al momento della sottoscrizione, consiste nella data alla scadenza della quale il file chiave perde di validità con conseguente disabilitazione dell'opzione di attivazione della licenza ad esso associata.

Di seguito è fornito un esempio di come il periodo di validità del file chiave è collegato al periodo di validità della licenza.

Esempio:

Periodo di validità della licenza: 300 giorni

Data di sottoscrizione del file chiave: 01.09.2009

Periodo di validità del file chiave: 300 giorni

Data di installazione del file chiave (attivazione della licenza): 10.09.2009, ossia 9 giorni dopo la data di sottoscrizione.

Risultato:

Periodo di validità della licenza calcolato: 300 giorni – 9 giorni = 291 giorni.

VISUALIZZAZIONE DELLE INFORMAZIONI SULLA LICENZA

È possibile visualizzare le seguenti informazioni sulla licenza: file chiave, tipo, numero di giorni mancanti alla scadenza e numero del dispositivo.

➧ *Per visualizzare le informazioni sulla licenza:*

1. Nella scheda **Avanzate**, selezionare **Licenza**.

   Verrà aperta la finestra **Licenza**.

2. Selezionare l'opzione **Info licenza** (vedere la figura sotto).

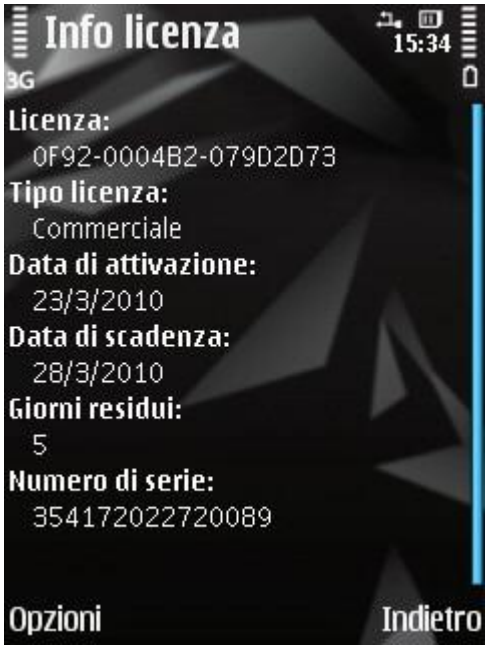


Figura 8. Visualizzazione delle informazioni sulla licenza

Verrà aperta la finestra **Informazioni sulla licenza**.

RINNOVO DELLA LICENZA

Kaspersky Mobile Security 9.0 consente di estendere la licenza dell'applicazione.

La licenza può essere estesa in uno dei seguenti modi:

- **Online**: attivando la licenza con una durata di un anno tramite il sito Web dedicato.
- **Tramite il codice di attivazione**, attivando l'applicazione con il codice di attivazione. È possibile acquistare il codice di attivazione su http://www.kasperskystore.it/cata_home.html oppure presso il proprio rivenditore Kaspersky Lab locale.

Per attivare l'applicazione sul proprio dispositivo mobile è necessario disporre di una connessione Internet configurata.

IN QUESTA SEZIONE

Rinnovo della licenza tramite il codice di attivazione 31

Rinnovo della licenza online 32

RINNOVO DELLA LICENZA TRAMITE IL CODICE DI ATTIVAZIONE

➡ *Per rinnovare la licenza tramite il codice di attivazione:*

1. Nella scheda **Avanzate**, selezionare **Licenza**.

   Verrà aperta la finestra **Licenza**.

2. Selezionare **Immetti codice**.

   Verrà aperta la finestra **Immetti codice**.

3. Successivamente, immettere il codice di attivazione ricevuto nei quattro campi, quindi selezionare **Opzioni** → **Attiva** (vedere la figura sotto).

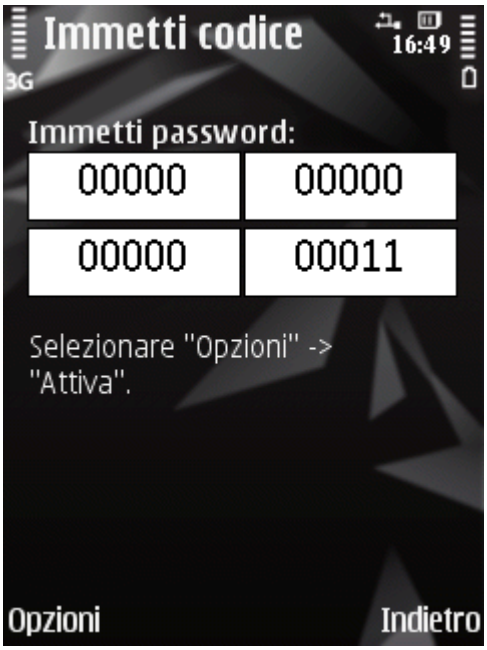


Figura 9. Rinnovo della licenza tramite il codice di attivazione

4. Se l'applicazione richiede un punto di accesso , selezionare il tipo di connessione richiesta dall'elenco dei suggerimenti.

   L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e scaricherà e installerà il file chiave. Se il file chiave viene installato correttamente, sullo schermo verranno visualizzate informazioni sulla licenza.

   Se per qualche motivo il codice di attivazione immesso non risulta valido, sullo schermo verrà visualizzato un messaggio corrispondente.

5. Al completamento dell'operazione, premere **OK**.

RINNOVO DELLA LICENZA ONLINE

➧ *Per rinnovare la licenza online:*

1. Nella scheda **Avanzate**, selezionare **Licenza**.

   Verrà aperta la finestra **Licenza**.

2. Selezionare **Rinnova online** (vedere la figura sotto).

Se il periodo di validità è scaduto, la voce del menu cambia in **Acquista online**.

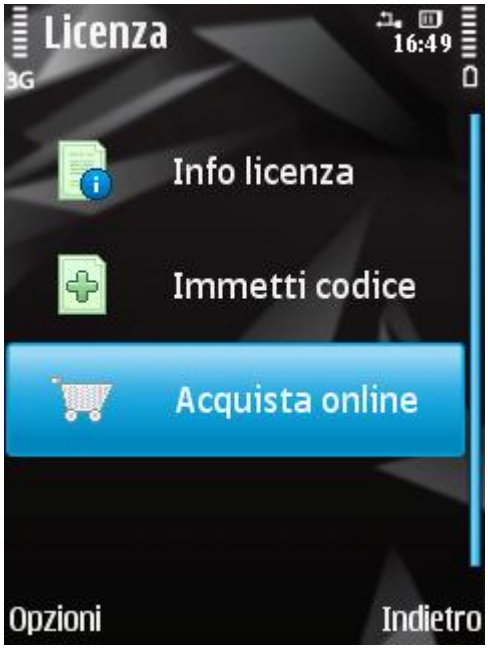


Figura 10. Rinnovo della licenza online

Verrà aperta la finestra **Acquista online**.

3. Premere **Apri**.

   Verrà aperto il sito Web http://www.kasperskystore.it in cui verrà chiesto di effettuare un ordine per il rinnovo della licenza.

   Se il periodo di validità è scaduto, verrà aperto il sito Web in cui è possibile acquistare il codice di attivazione online.

4. Seguire le istruzioni dettagliate.

5. Al termine dell'acquisto del codice di attivazione, immettere il codice di attivazione ricevuto (vedere la sezione "Rinnovo della licenza tramite il codice di attivazione" a pagina 31).

INTERFACCIA DELL'APPLICAZIONE

L'interfaccia di Kaspersky Mobile Security 9.0 è semplice e di facile utilizzo. Questa sezione fornisce informazioni sui suoi elementi principali.

ICONA PROTEZIONE

L'icona Protezione visualizza lo stato dell'applicazione. Se l'icona è attiva (a colori), la protezione è attivata. Se l'icona non è attiva (grigia), la protezione è stata arrestata e tutti i suoi componenti sono disattivati.

Per impostazione predefinita, l'icona Protezione non viene visualizzata sullo schermo del dispositivo. È possibile modificare le impostazioni di visualizzazione dell'icona (vedere la sezione "Visualizzazione dell'icona Protezione" a pagina 107).

FINESTRA STATO DI PROTEZIONE

Lo stato dei componenti principali dell'applicazione viene visualizzato nella finestra di stato corrente.

Per ciascun componente vi sono tre stati possibili, ognuno dei quali viene visualizzato con un colore specifico simile a quello dei semafori stradali. Il colore verde indica che la protezione del dispositivo è al livello necessario. I colori giallo e rosso indicano che vi sono vari livelli di minaccia della sicurezza. Le minacce non sono causate solo da programmi malware, ma derivano anche da database dell'applicazione obsoleti, dalla disabilitazione di alcuni componenti di protezione, da impostazioni di funzionamento dell'applicazione minime, ecc.

La finestra di stato è accessibile immediatamente dopo aver avviato l'applicazione e contiene le seguenti informazioni:

- **Protezione** è lo stato della protezione nella modalità di protezione in tempo reale (vedere la sezione "Protezione del file system" a pagina 36).

  L'icona di stato verde indica che la protezione è attiva e garantita al livello richiesto, e che i database dell'applicazione sono aggiornati.

  L'icona di colore giallo indica che i database non sono stati aggiornati da vari giorni.

  L'icona di colore rosso indica problemi che possono causare perdita di informazioni o infezione del dispositivo. Ad esempio, la protezione è disattivata. L'applicazione potrebbe non essere stata aggiornata da molto tempo.

- **Firewall** è il livello di protezione del dispositivo da attività di rete indesiderate (vedere la sezione "Filtro dell'attività di rete. Firewall" a pagina 89).

  L'icona di stato verde indica che il componente è attivo. Il livello di protezione del Firewall è selezionato.

  L'icona di colore rosso indica che l'attività di rete non è filtrata.

- **Antifurto** è lo stato di protezione in caso di smarrimento o furto del dispositivo (vedere la sezione "Protezione dei dati in caso di smarrimento o furto del dispositivo" a pagina 71).

  L'icona di stato verde indica che la funzione Antifurto è attiva; il nome della funzione è visualizzato solo lo stato del componente.

  L'icona di colore rosso indica che tutte le funzioni di Antifurto sono disabilitate.

- **Protezione privacy** è lo stato di protezione dei dati riservati (vedere la sezione "Mascheramento dei dati personali" a pagina 81).

  L'icona di stato verde indica che il componente è attivo. I dati riservati sono nascosti.

  L'icona di colore giallo avvisa il componente è disabilitato. I dati personali sono visualizzati e accessibili per la visualizzazione.

- **Licenza** è il periodo divalidità della licenza (vedere la sezione "Gestione della licenza" a pagina 28).

  L'icona di stato verde indica che il periodo di validità della licenza scadrà tra più di 14 giorni.

  L'icona di stato gialla indica che il periodo di validità della licenza scadrà tra meno di 14 giorni.

L'icona di colore rosso indica che la licenza è scaduta.

Figura 11. Finestra Stato corrente

È possibile anche accedere alla finestra di stato selezionando **Opzioni** → **Stato di protezione**.

Per impostazione predefinita, la finestra di stato viene visualizzata immediatamente dopo aver avviato l'applicazione. È possibile modificare le impostazioni di visualizzazione (vedere la sezione "Visualizzazione della finestra di stato" a pagina 106).

SCHEDE DELL'APPLICAZIONE

I componenti dell'applicazione sono organizzati in gruppi logici e sono accessibili tramite schede. Ogni scheda consente di accedere alle impostazioni del componente selezionato e alle operazioni di protezione.

Il menu di Kaspersky Mobile Security 9.0 contiene le seguenti schede:

- **Anti-Virus**: protezione del file system, scansione manuale e aggiornamento dei database dell'applicazione.
- **Protezione privacy**: mascheramento dei dati riservati sul dispositivo.
- **Antifurto**: blocco del dispositivo e cancellazione dei dati in caso di smarrimento o furto.
- **Criptaggio**: protezione delle informazioni sul dispositivo tramite crittografia.
- **Anti-Spam**: filtro delle chiamate e dei messaggi SMS in entrata indesiderati.
- **Parental Control**: controllo delle chiamate e dei messaggi SMS in uscita.
- **Firewall**: protezione del dispositivo quando è connesso a una rete.
- **Avanzate**: impostazioni generali dell'applicazione, dettagli sull'applicazione, sui database utilizzati e sulla licenza.

Per impostazione predefinita, le schede dell'applicazione sono accessibili dopo la visualizzazione della finestra di stato (vedere la sezione "Finestra Stato di protezione" a pagina 34).

È possibile navigare tra le schede nei seguenti modi:

- utilizzando i pulsanti di spostamento del dispositivo;
- selezionando **Opzioni** → **Apri scheda**.

MENU DELL'APPLICAZIONE

Il menu dell'applicazione consente di eseguire le operazioni principali. Il menu contiene le seguenti voci (vedere la figura sotto):

- **Selezione**: selezione di opzioni, comandi o impostazioni.
- **Apri scheda**: consente di selezionare un componente dell'applicazione.
- **Stato di protezione**: consente di visualizzare la finestra Stato di protezione corrente.
- **Guida**: richiama la guida rapida di Kaspersky Mobile Security 9.0.
- **Info**: apre una finestra che visualizza i dettagli del programma.
- **Esci**: chiude Kaspersky Mobile Security 9.0.

Figura 12. Menu del programma

➡ *Per aprire il menu dell'applicazione,*

selezionare **Opzioni**.

Per spostarsi tra le voci del menu dell'applicazione, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

PROTEZIONE DEL FILE SYSTEM

Questa sezione fornisce informazioni sul componente Protezione che consente di evitare le infezioni del file system del dispositivo. La sezione spiega inoltre come attivare/arrestare il componente Protezione e regolare le sue impostazioni di funzionamento.

IN QUESTA SEZIONE

Informazioni sul componente Protezione....37

Abilitazione e disabilitazione del componente Protezione....37

Configurazione dell'area di protezione....38

Selezione dell'azione da eseguire sugli oggetti rilevati....39

Ripristino delle impostazioni di protezione predefinite....40

INFORMAZIONI SUL COMPONENTE PROTEZIONE

Il componente Protezione viene caricato all'avvio del sistema operativo del dispositivo e rimane residente nella memoria del dispositivo, sottoponendo a scansione tutti i file aperti, salvati o eseguiti. I file vengono sottoposti a scansione mediante il seguente algoritmo:

1. Il componente intercetta ogni tentativo di accesso a qualsiasi file da parte dell'utente o di qualunque programma.

2. Il file viene sottoposto a scansione per verificare la presenza di eventuali oggetti nocivi (malware). Gli oggetti nocivi vengono rilevati mediante confronto con i database dell'applicazione, che contengono le descrizioni di tutti gli oggetti nocivi noti e i metodi per neutralizzarli.

3. Dopo l'analisi, Kaspersky Mobile Security 9.0 può eseguire le seguenti azioni correttive:

   - Se all'interno del file è stato rilevato del codice dannoso, l'applicazione blocca l'accesso al file ed esegue l'azione specificata nelle impostazioni.

   - Se nel file non viene rilevato alcun codice dannoso, il file verrà immediatamente ripristinato.

Le informazioni sui risultati della scansione vengono salvate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

ABILITAZIONE E DISABILITAZIONE DEL COMPONENTE PROTEZIONE

Quando si attiva il componente Protezione, tutte le operazioni eseguite sul sistema sono costantemente sotto controllo. Per assicurare la protezione da oggetti nocivi, vengono utilizzate le risorse del dispositivo. Per ridurre il carico di lavoro sul dispositivo durante l'esecuzione di più attività, è possibile arrestare temporaneamente il componente Protezione.

Gli esperti di Kaspersky Lab consigliano di non disabilitare il componente Protezione, in quanto ciò può causare l'infezione del computer e perdita di dati.

Lo stato corrente del componente Protezione è visualizzato nella scheda **Anti-Virus** accanto alla voce del menu **Protezione**.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per abilitare il componente Protezione:

1. Selezionare l'opzione **Protezione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Protezione**.

2. Selezionare per l'impostazione **Modalità Protezione** il valore **Abilitato** (vedere la figura sotto).

Figura 13. Abilitazione del componente Protezione

3. Premere **Indietro** per salvare le modifiche.

Per disabilitare il componente Protezione:

1. Selezionare l'opzione **Protezione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Protezione**.

2. Selezionare per l'impostazione **Modalità Protezione** il valore **Disabilitato**.

3. Premere **Indietro** per salvare le modifiche.

CONFIGURAZIONE DELL'AREA DI PROTEZIONE

Per impostazione predefinita, Kaspersky Mobile Security 9.0 sottopone a scansione tutti i tipi di file. Per limitare il tempo necessario alla verifica, è possibile impostare il tipo di oggetti da sottoporre a scansione.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per selezionare il tipo di oggetti da sottoporre a scansione:

1. Selezionare l'opzione **Protezione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Protezione**.

2. Selezionare un valore per l'impostazione **Oggetti da analizzare** (vedere la figura sotto):

   - **Tutti i file**: esegue la scansione di tutti i tipi di file.

- **Eseguibili**: esegue solo la scansione dei file di programma eseguibili (ad esempio *.exe, *.sis, *.mdl, *.app).

Figura 14. Selezione degli oggetti da sottoporre a scansione

3. Premere **OK** per salvare le modifiche.

SELEZIONE DELL'AZIONE DA ESEGUIRE SUGLI OGGETTI RILEVATI

Per impostazione predefinita, Kaspersky Mobile Security 9.0 sposta gli oggetti nocivi rilevati in quarantena. È possibile cambiare l'azione che l'applicazione deve eseguire se viene rilevato un oggetto nocivo.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per configurare la risposta dell'applicazione quando viene rilevato un oggetto malware:

1. Selezionare l'opzione **Protezione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Protezione**.

2. Specificare l'azione che l'applicazione deve eseguire se viene rilevato un oggetto nocivo. Per eseguire questa operazione, selezionare un valore per l'impostazione **Se viene rilevato un virus** (vedere la figura sotto):

   - **Elimina**: elimina gli oggetti malware senza avvisare l'utente.
   - **Quarantena**: mette in quarantena gli oggetti malware.

- **Registra evento**: non elabora gli oggetti malware e registra le informazioni sul loro rilevamento nel report dell'applicazione. Blocca l'oggetto se si tenta di utilizzarlo (ad esempio, per copiarlo o aprirlo).

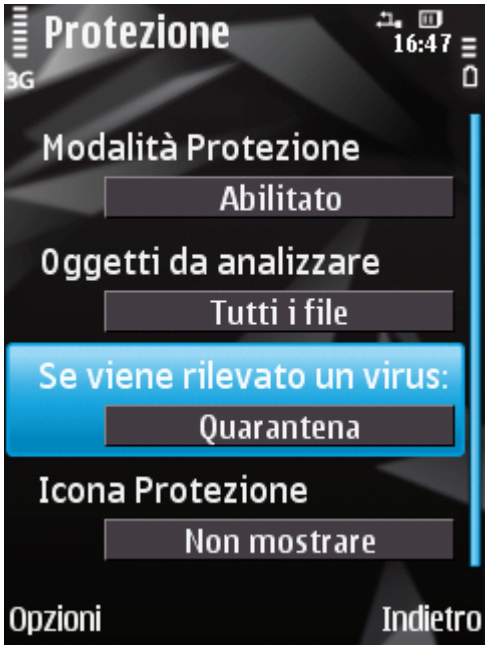


Figura 15. Risposta del programma verso un oggetto nocivo rilevato

3. Premere **OK** per salvare le modifiche.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE PREDEFINITE

Per impostazione predefinita, il componente Protezione funziona con le impostazioni consigliate dagli esperti di Kaspersky Lab. Durante l'impostazione del componente Protezione, è sempre possibile ripristinare i parametri di funzionamento consigliati.

Per ripristinare le impostazioni di protezione predefinite:

1. Selezionare l'opzione **Protezione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Protezione**.

2. Selezionare **Opzioni** → **Ripristina**.

SCANSIONE DEL DISPOSITIVO

Questa sezione fornisce informazioni sulla scansione anti-virus che consente di rilevare e neutralizzare le minacce nel dispositivo. La sezione specifica inoltre come eseguire l'attività di scansione, come pianificare l'esecuzione delle attività, come selezionare gli oggetti da sottoporre a scansione e come specificare l'azione dell'applicazione su una minaccia rilevata.

IN QUESTA SEZIONE

Informazioni sulla scansione del dispositivo 41

Avvio di una scansione manuale 41

Avvio di una scansione pianificata 43

Selezione del tipo di oggetti da sottoporre a scansione 44

Selezione dell'azione da eseguire sugli oggetti rilevati 45

Configurazione della scansione degli archivi 47

Ripristino delle impostazioni predefinite di scansione del dispositivo 48

INFORMAZIONI SULLA SCANSIONE DEL DISPOSITIVO

La scansione del dispositivo facilita il rilevamento e la neutralizzazione di eventuali oggetti nocivi presenti nel dispositivo. Kaspersky Mobile Security 9.0 consente di eseguire una scansione completa o parziale del file system del dispositivo, ossia solo la scansione del contenuto della memoria del dispositivo, dei messaggi o di una cartella specifica (incluse le cartelle presenti nella scheda di memoria).

La procedura di scansione del dispositivo è la seguente:

1. Kaspersky Mobile Security 9.0 esegue la scansione dei tipi di file selezionati (vedere la sezione "Selezione dei tipi di oggetti da sottoporre a scansione" a pagina 44).

2. Il file viene sottoposto a scansione per verificare la presenza di eventuali oggetti nocivi (malware). Kaspersky Mobile Security 9.0 rileva gli oggetti nocivi in base ai database dell'applicazione, che contengono le descrizioni di tutti gli oggetti nocivi noti e i metodi per neutralizzarli.

   Dopo l'analisi, Kaspersky Mobile Security 9.0 può eseguire le seguenti azioni correttive:

   - se viene rilevato un oggetto nocivo nel file, Kaspersky Mobile Security 9.0 esegue l'attività specificata (vedere la sezione "Selezione di un'azione da eseguire sugli oggetti" a pagina 45);

   - se non viene rilevato alcun codice dannoso, il file diventa immediatamente accessibile per l'uso.

Un'attività di scansione può essere avviata manualmente o automaticamente in base a una pianificazione definita precedentemente (vedere la sezione "Avvio di una scansione pianificata" a pagina 43).

Le informazioni sui risultati della scansione manuale vengono salvate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

AVVIO DI UNA SCANSIONE MANUALE

È possibile avviare una scansione manualmente in qualsiasi momento. Il momento migliore è tuttavia quando il processore del dispositivo non è impegnato ad eseguire altre operazioni.

Per avviare manualmente una scansione anti-virus:

1. Selezionare **Scansione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Scansione**.

2. Selezionare l'area di scansione del dispositivo (vedere la figura sotto):

- **Scansione compl.**: esegue la scansione dell'intero file system del dispositivo. Per impostazione predefinita, vengono sottoposti a scansione i seguenti oggetti: memoria del dispositivo e scheda di memoria.

- **Scansione cartella**: esegue la scansione di un determinato oggetto nel file system del dispositivo o sulla scheda di memoria. Se si seleziona l'opzione **Scansione cartella**, verrà aperta una finestra che visualizza il file system del dispositivo. Utilizzare i pulsanti di spostamento per spostarsi nel file system. Per avviare la scansione della cartella, selezionare la cartella desiderata e selezionare **Opzioni** → **Scansione**.

- **Scansione mem.**: esegue la scansione dei processi avviati nella memoria di sistema e dei file corrispondenti.

- **Scansione msg**: esegue la scansione dei messaggi ricevuti tramite SMS, MMS o Bluetooth.

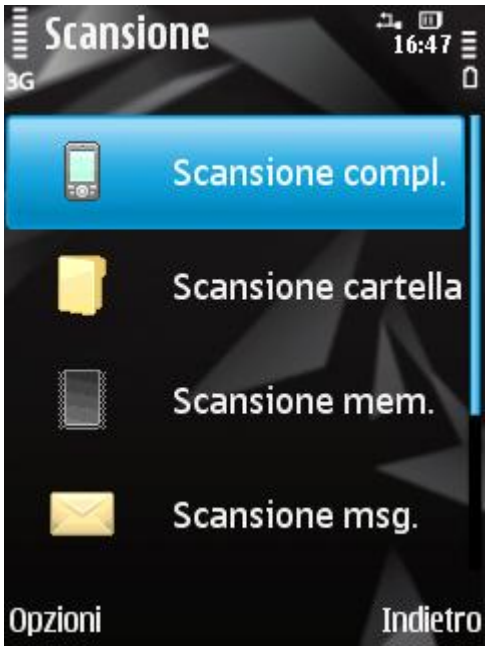


Figura 16. Selezione dell'area di scansione

Dopo aver avviato la scansione, si aprirà una finestra del processo di scansione che indica lo stato corrente: numero di oggetti sottoposti a scansione, percorso dell'oggetto sottoposto a scansione e un indicatore dei risultati della scansione in percentuale (vedere la figura sotto).

Figura 17. Stato della scansione del dispositivo

Se Kaspersky Mobile Security 9.0 rileva un oggetto infetto, esegue un'azione in base ai parametri di scansione impostati (vedere la sezione "Selezione di un'azione da eseguire sugli oggetti" a pagina 45).

Per impostazione predefinita, se Kaspersky Mobile Security 9.0 rileva una minaccia, tenta di eliminarla. Se questo non è possibile, il programma sposta l'oggetto infetto in quarantena.

Al termine della scansione, sullo schermo vengono visualizzate statistiche complessive con le seguenti informazioni:

- numero di oggetti sottoposti a scansione;
- numero di virus rilevati, messi in quarantena o eliminati;
- numero di oggetti ignorati (ad esempio, file bloccati dal sistema operativo o file non eseguibili, durante la scansione dei soli file di programma eseguibili);
- ora della scansione.

Per risparmiare carica della batteria, per impostazione predefinita la retroilluminazione dello schermo viene disabilitata automaticamente durante la scansione. È possibile modificare le impostazioni della retroilluminazione dello schermo (vedere la sezione "Gestione della retroilluminazione" a pagina 106).

AVVIO DI UNA SCANSIONE PIANIFICATA

Kaspersky Mobile Security 9.0 consente la creazione di una pianificazione di ore in cui le scansioni verranno avviate automaticamente. Le scansioni vengono eseguite in background. Quando viene rilevato un oggetto infetto, su di esso verrà eseguita l'azione selezionata nelle **Impostazioni di scansione**.

Per impostazione predefinita, l'avvio di una scansione pianificata è disabilitato.

➧ *Per impostare una scansione pianificata:*

1. Selezionare l'opzione **Scansione** nella scheda **Anti-Virus**.

Verrà aperta la finestra **Scansione**.

2. Selezionare l'opzione **Pianifica**.

   Verrà aperta la finestra **Pianifica**.

3. Impostare un valore per l'impostazione **Scansione automatica** (vedere la figura sotto):

   - **Disabilitato**: disabilita le scansioni pianificate.
   - **Settimanale**: esegue la scansione una volta alla settimana. Specificare il **Giorno scansione** e l'**Ora scansione** per impostare il giorno della settimana e l'ora del giorno in cui verrà avviata la scansione.
   - **Giornaliero**: esegue la scansione ogni giorno. Specificare l'**Ora scansione** nel campo di immissione per impostare l'ora del giorno in cui verrà avviata la scansione.

Figura 18. Configurazione di una scansione pianificata

4. Premere **Indietro** per salvare le modifiche.

SELEZIONE DEL TIPO DI OGGETTI DA SOTTOPORRE A SCANSIONE

Per impostazione predefinita, Kaspersky Mobile Security 9.0 sottopone a scansione tutti i file salvati nel dispositivo e sulla scheda di memoria. Per ridurre il tempo di scansione, è possibile selezionare i tipi di oggetti da sottoporre a scansione, ossia determinare quali formati di file l'applicazione deve sottoporre a scansione per rilevare codice dannoso.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per selezionare gli oggetti da sottoporre a scansione:

1. Selezionare l'opzione **Scansione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Scansione**.

2. Selezionare **Oggetti/azioni**.

Verrà aperta la finestra **Oggetti e azioni**.

3. Selezionare un valore per le impostazioni **Oggetti da analizzare** (vedere la figura sotto):

   - **Tutti i file**: esegue la scansione di tutti i tipi di file, nonché decomprime e sottopone a scansione il contenuto degli archivi. Vengono sottoposti a scansione gli archivi nei seguenti formati: *.zip, *.sis, *.cab e *.sisx.

   - **Eseguibili**: esegue solo la scansione dei file di programma dei seguenti formati: *.exe, *.dll, *.sis, *.mdl, *.app, *.rdl, *.prt, *.pxt, *.ldd, *.pdd, *.class. Inoltre, gli archivi non vengono decompressi e sottoposti a scansione.

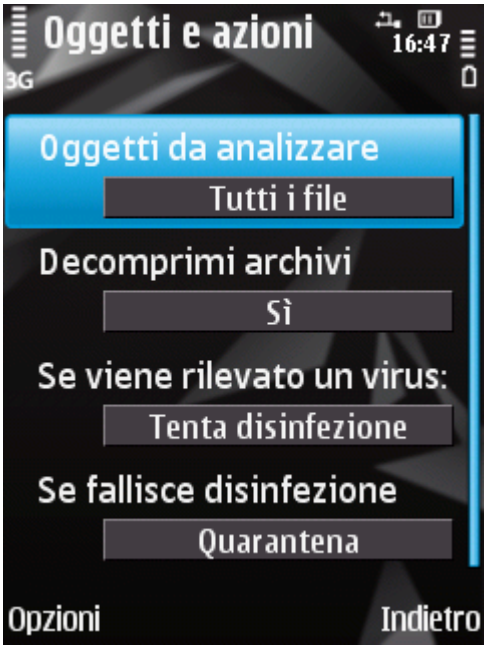


Figura 19. Selezione del tipo di file da sottoporre a scansione

4. Premere **Indietro** per salvare le modifiche.

SELEZIONE DELL'AZIONE DA ESEGUIRE SUGLI OGGETTI RILEVATI

Per impostazione predefinita, Kaspersky Mobile Security 9.0 sposta gli oggetti infetti rilevati in quarantena. È possibile specificare quali azioni eseguirà l'applicazione quando rileva un oggetto nocivo.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per configurare la risposta dell'applicazione:

1. Selezionare **Scansione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Scansione**.

2. Selezionare **Oggetti/azioni**.

   Verrà aperta la finestra **Oggetti e azioni**.

3. Specificare l'azione da eseguire nei confronti di un oggetto nocivo. Per eseguire questa operazione, selezionare un valore per l'impostazione **Se viene rilevato un virus** (vedere la figura sotto):

- **Elimina**: elimina gli oggetti malware rilevati senza avvisare l'utente.
- **Quarantena**: mette in quarantena gli oggetti nocivi rilevati.
- **Chiedi a utente**: richiede all'utente quale azione eseguire. Quando viene rilevata una minaccia, visualizza un messaggio di notifica con una richiesta di intervento dell'utente.
- **Registra evento**: non elabora gli oggetti malware e registra le informazioni sul loro rilevamento nel report dell'applicazione. Blocca l'oggetto se si tenta di utilizzarlo (ad esempio, per copiarlo o aprirlo).
- **Tenta disinfezione**: tenta di disinfettare gli oggetti malware. Se la disinfezione non è possibile, viene eseguita l'azione specificata per l'impostazione **Se fallisce disinfezione**.

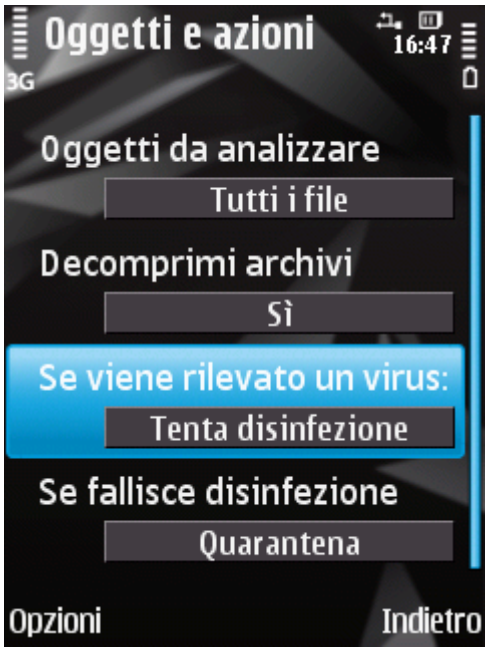


Figura 20. Selezione dell'azione da eseguire sugli oggetti nocivi

4. Se è stata selezionata l'opzione **Tenta disinfezione**, impostare una seconda azione da far eseguire all'applicazione se l'oggetto non può essere disinfettato. Per eseguire questa operazione, selezionare un valore per l'impostazione **Se fallisce disinfezione** (vedere la figura sotto):

    - **Elimina**: elimina gli oggetti malware senza avvisare l'utente.
    - **Quarantena**: mette in quarantena gli oggetti.
    - **Chiedi a utente**: richiede all'utente quale azione eseguire quando viene rilevato un oggetto nocivo.

- **Registra evento**: non elabora gli oggetti malware e registra le informazioni sul loro rilevamento nel report dell'applicazione. Blocca l'oggetto se si tenta di utilizzarlo (ad esempio, per copiarlo o aprirlo).

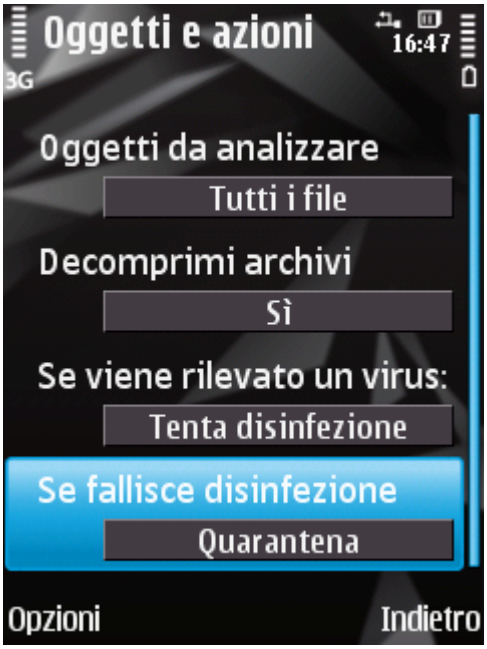


Figura 21. Selezione dell'azione da eseguire sugli oggetti nocivi, se la disinfezione non è possibile

5. Premere **Indietro** per salvare le modifiche.

CONFIGURAZIONE DELLA SCANSIONE DEGLI ARCHIVI

I virus si nascondono spesso negli archivi. Per eseguire la scansione del contenuto degli archivi, è necessario decomprimerli. Ciò può ridurre in modo significativo la velocità di scansione del dispositivo.

Per impostazione predefinita, la decompressione degli archivi è abilitata. L'applicazione esegue la scansione degli archivi nei seguenti formati: *.zip, *.sis, *.cab e *.sisx. Per aumentare la velocità della scansione è possibile disabilitare la decompressione degli archivi.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

➧ *Per disabilitare la decompressione degli archivi:*

1. Selezionare l'opzione **Scansione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Scansione**.

2. Selezionare **Oggetti/azioni**.

   Verrà aperta la finestra **Oggetti e azioni**.

3. Per l'impostazione **Decomprimi archivi**, selezionare il valore **No** (vedere la figura sotto).

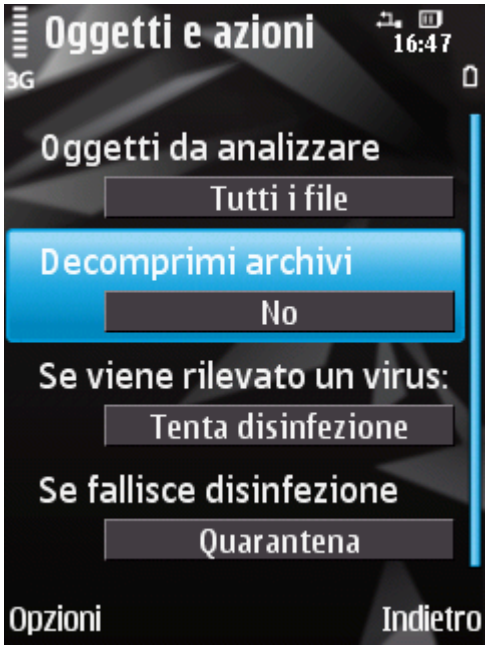


Figura 22. Configurazione della scansione degli archivi

4. Premere **Indietro** per salvare le modifiche.

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE DI SCANSIONE DEL DISPOSITIVO

Per impostazione predefinita, la scansione del dispositivo viene eseguita con i valori di impostazione consigliati dagli esperti di Kaspersky Lab. Durante l'impostazione della scansione del dispositivo, è sempre possibile ripristinare i parametri di funzionamento consigliati.

➧ *Per ripristinare le impostazioni predefinite di scansione del dispositivo:*

1. Selezionare l'opzione **Scansione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Scansione**.

2. Selezionare **Oggetti/azioni**.

   Verrà aperta la finestra **Oggetti e azioni**.

3. Selezionare **Opzioni → Ripristina**.

QUARANTENA DEGLI OGGETTI POTENZIALMENTE INFETTI

Questa sezione fornisce informazioni sulla *quarantena*, una cartella speciale in cui vengono collocati gli oggetti potenzialmente nocivi. La sezione specifica inoltre come gestire gli oggetti in quarantena: come visualizzare, ripristinare o eliminare gli oggetti presenti in questa cartella.

IN QUESTA SEZIONE

Informazioni sulla Quarantena 49

Visualizzazione di oggetti in quarantena 49

Ripristino di oggetti dalla quarantena 50

Eliminazione di oggetti dalla quarantena 50

INFORMAZIONI SULLA QUARANTENA

La Quarantena è una cartella specifica in cui Kaspersky Mobile Security 9.0 colloca gli oggetti potenzialmente nocivi.

Gli oggetti nocivi possono essere rilevati e messi in quarantena durante una scansione del dispositivo oppure durante il funzionamento di Protezione.

Gli oggetti messi in quarantena vengono memorizzati in un formato compresso che ne impedisce l'attivazione e neutralizza la potenziale minaccia al dispositivo. Gli oggetti messi in quarantena possono essere eliminati o ripristinati dall'utente.

VISUALIZZAZIONE DI OGGETTI IN QUARANTENA

È possibile visualizzare gli oggetti messi in quarantena. Per ogni oggetto vengono specificati il nome completo e la data di rilevamento.

- *Per visualizzare l'elenco degli oggetti in quarantena:*

  selezionare l'opzione **Quarantena** nella scheda **Anti-Virus**.

Verrà aperta la finestra **Quarantena** contenente un elenco degli oggetti memorizzati nella Quarantena (vedere la figura sotto).

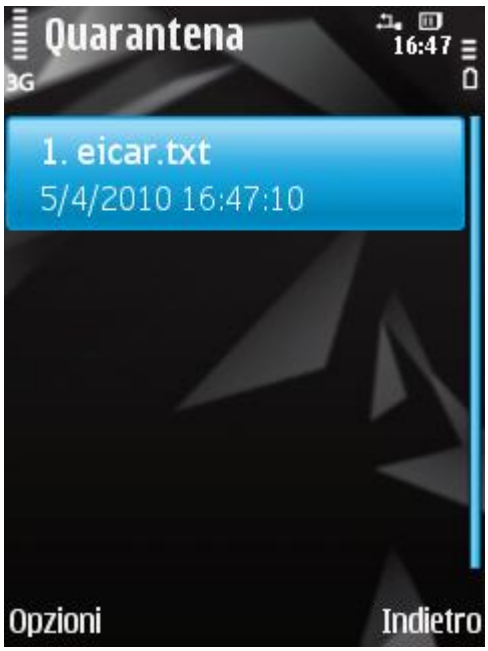


Figura 23. Elenco di oggetti in quarantena

RIPRISTINO DI OGGETTI DALLA QUARANTENA

Se si è sicuri che l'oggetto in quarantena non rappresenta una minaccia per il dispositivo, è possibile ripristinarlo dalla quarantena. L'oggetto ripristinato viene rimesso nella cartella originale.

- *Per ripristinare un oggetto dalla quarantena:*

1. Selezionare l'opzione **Quarantena** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Quarantena**.

2. Selezionare l'oggetto che si desidera ripristinare e selezionare **Opzioni→ Ripristina**.

ELIMINAZIONE DI OGGETTI DALLA QUARANTENA

È possibile eliminare uno o tutti gli oggetti memorizzati nella quarantena.

- *Per eliminare un oggetto dalla quarantena:*

1. Selezionare l'opzione **Quarantena** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Quarantena**.

2. Selezionare l'oggetto che si desidera eliminare e selezionare **Opzioni→ Elimina**.

L'oggetto selezionato verrà eliminato.

- *Per eliminare tutti gli oggetti in quarantena:*

1. Selezionare l'opzione **Quarantena** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Quarantena**.

2. Selezionare **Opzioni→ Elimina tutto**.

Tutti gli oggetti in quarantena verranno eliminati.

FILTRO DELLE CHIAMATE E DEI MESSAGGI SMS IN ENTRATA

Questa sezione fornisce informazioni sul componente Anti-Spam che filtra i messaggi e le chiamate in entrata in base alla Lista bloccati e alla Lista consentiti. La sezione specifica inoltre come creare la Lista bloccati e la Lista consentiti, come selezionare un'azione di Anti-Spam nei confronti dei messaggi e delle chiamate in entrata e come configurare le impostazioni di funzionamento del componente.

IN QUESTA SEZIONE

Informazioni su Anti-Spam 51

Modalità Anti-Spam 52

Modifica della modalità Anti-Spam 52

Creazione di una Lista bloccati 53

Creazione di una Lista consentiti 56

Risposta ai messaggi SMS e alle chiamate da contatti non in rubrica 59

Risposta ai messaggi SMS da mittenti non numerici 60

Selezione di una risposta ai messaggi SMS in entrata 61

Selezione di una risposta alle chiamate in entrata 62

INFORMAZIONI SU ANTI-SPAM

Anti-Spam protegge il dispositivo dalla ricezione di chiamate e messaggi indesiderati. Anti-Spam filtra i messaggi SMS e le chiamate in entrata utilizzando la Lista bloccati e la Lista consentiti.

Le liste sono composte da voci. Ogni voce può contenere le seguenti impostazioni:

- tipo di dati (messaggio SMS, chiamate, messaggio SMS e chiamate) cui si applicano le impostazioni di filtro (impostazione obbligatoria);
- numero dell'abbonato da cui vengono ricevuti i dati;
- testo contenuto in un messaggio SMS.

Anti-Spam filtra i messaggi e le chiamate in base alle impostazioni selezionate (vedere la sezione "Modalità Anti-Spam" a pagina 52). In base a queste impostazioni, Anti-Spam esegue la scansione di ogni messaggio SMS o chiamata in entrata e determina se il messaggio o la chiamata è desiderata o indesiderata (spam). Non appena Anti-Spam assegna lo stato di desiderato o indesiderato a un messaggio SMS o a una chiamata, la scansione termina.

Per impostazione predefinita, l'algoritmo di Anti-Spam è composto dai seguenti passaggi:

1. Scansione dei messaggi SMS in entrata per verificare se sono identici al numero dell'abbonato e al testo:
   a. Dalla Lista bloccati. Se nella lista viene trovata una voce in cui il numero e il testo sono identici ai dati del messaggio SMS in entrata, il messaggio SMS viene considerato come indesiderato e bloccato. Il programma elimina il messaggio SMS bloccato.
   b. Dalla Lista consentiti. Se nella lista viene trovata una voce in cui il numero e il testo sono identici ai dati del messaggio SMS in entrata, il messaggio SMS viene considerato come desiderato e consentito.
2. Scansione delle chiamate e dei messaggi SMS per verificare la conformità solo rispetto al numero:
   a. Dalla Lista bloccati. Se nella lista viene trovata una voce in cui il numero è identico al numero del mittente (mentre il testo non è stato specificato nella voce), la chiamata o il messaggio SMS viene considerato come spam e bloccato. Il programma elimina il messaggio SMS bloccato.
   b. Dalla Lista consentiti. Se nella lista viene trovata una voce in cui il numero è identico al numero del mittente (mentre il testo non è stato specificato nella voce), la chiamata o il messaggio SMS viene considerato come desiderato e consentito.

3. Scansione dei messaggi per verificare la conformità solo rispetto al testo:

   a. Dalla Lista bloccati. Se nella lista viene trovata una voce in cui il testo è identico ai dati del messaggio SMS in entrata (mentre il numero non è stato specificato nella voce), il messaggio SMS viene considerato come spam e bloccato. Il programma elimina il messaggio SMS bloccato.

   b. Dalla Lista consentiti. Se nella lista viene trovata una voce in cui il testo è identico ai dati del messaggio SMS in entrata (mentre il numero non è stato specificato nella voce), il messaggio SMS viene considerato come desiderato e consentito.

4. Selezione di un'azione. Se non viene trovata alcuna conformità nella Lista bloccati o nella Lista consentiti, per impostazione predefinita Anti-Spam recapita le chiamate e i messaggi SMS e suggerisce di eseguire un'azione nei confronti delle chiamate o dei messaggi nella finestra di notifica. È possibile inoltre visualizzare informazioni aggiuntive nella notifica. Per le chiamate ricevute viene indicato il numero del chiamante. Per i messaggi SMS vengono visualizzati il numero dell'abbonato e il contenuto.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

MODALITÀ ANTI-SPAM

Per modalità Anti-Spam si intende una configurazione di base, o una raccolta di parametri, del componente che protegge il dispositivo da chiamate e messaggi indesiderati.

Sono disponibili le seguenti modalità Anti-Spam:

- **Entrambe le liste**: filtra i messaggi SMS e le chiamate in entrata utilizzando entrambe la Lista bloccati e la Lista consentiti. Quando viene ricevuto un messaggio SMS o una chiamata da un numero di telefono non presente in nessuna delle liste, l'utente riceverà una notifica. Verrà chiesto quindi di selezionare un'azione: consentire il messaggio SMS o la chiamata senza aggiungere il numero di telefono dell'abbonato alle liste oppure aggiungere il numero di telefono alla Lista bloccati o alla Lista consentiti.

  Questa è la modalità predefinita.

- **Lista bloccati**: blocca i messaggi SMS e le chiamate corrispondenti alle voci nella Lista bloccati. I messaggi SMS bloccati vengono eliminati. Tutti gli altri messaggi SMS e le chiamate vengono recapitati.

- **Lista consentiti**: recapita i messaggi SMS e le chiamate corrispondenti alle voci nella Lista consentiti. Tutti gli altri messaggi SMS e le chiamate verranno bloccati. I messaggi SMS bloccati vengono eliminati.

- **Disabilitato**: non filtra i messaggi SMS e le chiamate.

È possibile modificare la modalità Anti-spam (vedere la sezione "Modifica della modalità Anti-Spam" a pagina 52). La modalità corrente di Anti-Spam è visualizzata nella scheda **Anti-Spam** accanto alla voce del menu **Modalità**.

MODIFICA DELLA MODALITÀ ANTI-SPAM

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per selezionare la modalità Anti-Spam, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Modalità** nella scheda **Anti-Spam**.

   Verrà aperta la finestra **Modalità**.

2. Selezionare un valore per l'impostazione **Modalità Anti-Spam** (vedere la figura sotto).

Figura 24. Modifica della modalità Anti-Spam

3. Premere **Indietro** per salvare le modifiche.

CREAZIONE DI UNA LISTA BLOCCATI

È possibile creare una Lista bloccati in base alla quale Anti-Spam blocca le chiamate e i messaggi SMS in entrata.

La lista contiene numeri di telefono e frasi la cui presenza in un messaggio SMS indica che si tratta di spam.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

IN QUESTA SEZIONE

Aggiunta di voci alla Lista bloccati 53

Modifica di voci nella Lista bloccati 55

Eliminazione di voci dalla Lista bloccati 56

Eliminazione di tutte le voci 56

AGGIUNTA DI VOCI ALLA LISTA BLOCCATI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri Anti-Spam. Se un numero è già stato salvato in una di queste liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per aggiungere una voce alla Lista bloccati:

1. Selezionare **Lista bloccati** nella scheda **Anti-Spam**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare **Opzioni→ Aggiungi voce** (vedere la figura sotto).

Figura 25. Aggiunta di voci alla Lista bloccati

3. Selezionare le seguenti impostazioni (vedere la figura sotto):

   - **Blocca in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà bloccato da Anti-Spam:

     - **Chiamate e SMS**: blocca i messaggi SMS e le chiamate in entrata.
     - **Solo chiamate**: blocca solo le chiamate in entrata.
     - **Solo SMS**: blocca solo i messaggi SMS in entrata.

   - **Da numero di telefono**: numero di telefono da cui la ricezione di messaggi SMS e/o di chiamate viene bloccata. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS è spam. L'impostazione è disponibile se per l'impostazione **Blocca in entrata** è impostato il valore **Solo SMS**.

Figura 26. Impostazioni della voce

4. Premere **Indietro** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA BLOCCATI

È possibile cambiare i valori di tutte le impostazioni relative ai numeri presenti nella Lista bloccati.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni → Cambia**.

Per modificare una voce della Lista bloccati di Anti-Spam:

1. Selezionare **Lista bloccati** nella scheda **Anti-Spam**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare dalla lista la voce che si desidera modificare e selezionare **Opzioni→ Modifica voce**.

3. Modificare le impostazioni relative alla voce necessarie:

   - **Blocca in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà bloccato da Anti-Spam:

     - **Chiamate e SMS**: blocca i messaggi SMS e le chiamate in entrata.

     - **Solo chiamate**: blocca solo le chiamate in entrata.

     - **Solo SMS**: blocca solo i messaggi SMS in entrata.

   - **Da numero di telefono**: numero di telefono da cui la ricezione di messaggi SMS e/o di chiamate viene bloccata. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS è spam. L'impostazione è disponibile se per l'impostazione **Blocca in entrata** è impostato il valore **Solo SMS**.

4. Premere **Indietro** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA BLOCCATI

In caso di aggiunta accidentale di un numero alla Lista bloccati è possibile eliminare tale numero dalla lista.

Per eliminare una voce dalla Lista bloccati di Anti-Spam:

1. Selezionare **Lista bloccati** nella scheda **Anti-Spam**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare dalla lista la voce da modificare e selezionare **Opzioni** → **Elimina voce**.

ELIMINAZIONE DI TUTTE LE VOCI

Per eliminare tutte le voci dalla Lista bloccati di Anti-Spam:

1. Selezionare **Lista bloccati** nella scheda **Anti-Spam**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare la voce del menu **Opzioni** → **Elimina tutte le voci**.

La lista verrà svuotata.

CREAZIONE DI UNA LISTA CONSENTITI

È possibile creare una Lista consentiti in base alla quale Anti-Spam consente le chiamate e i messaggi SMS in entrata.

La lista contiene i numeri di telefono dei mittenti e le frasi che non si considerano come spam.

IN QUESTA SEZIONE

Aggiunta di voci alla Lista consentiti 56

Modifica di voci nella Lista consentiti 58

Eliminazione di voci dalla Lista consentiti 59

Eliminazione di tutte le voci dalla Lista consentiti 59

AGGIUNTA DI VOCI ALLA LISTA CONSENTITI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri Anti-Spam. Se un numero è già stato salvato in una di queste liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per aggiungere una voce alla Lista consentiti di Anti-Spam:

1. Nella scheda **Anti-Spam**, selezionare **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare la voce del menu **Opzioni** → **Aggiungi voce** (vedere la figura sotto).

Figura 27. Aggiunta di voci alla Lista consentiti

3. Selezionare le seguenti impostazioni per la nuova voce (vedere la figura sotto):

   - **Consenti in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà consentito da Anti-Spam:

     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in entrata.

     - **Solo chiamate**: consente solo le chiamate in entrata.

     - **Solo SMS**: consente solo i messaggi SMS in entrata.

   - **Da numero di telefono**: numero di telefono per il quale la ricezione di messaggi SMS e/o di chiamate viene consentita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS non è spam. L'impostazione è disponibile se per l'impostazione **Consenti in entrata** è impostato il valore **Solo SMS**.

Figura 28. Impostazioni della voce

4. Premere **Indietro** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA CONSENTITI

È possibile cambiare i valori di tutte le impostazioni relative ai numeri presenti nella Lista consentiti.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

➧ *Per modificare una voce della Lista consentiti di Anti-Spam:*

1. Nella scheda **Anti-Spam**, selezionare **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare dalla lista la voce che si desidera modificare e selezionare la voce del menu **Opzioni** → **Modifica voce**.

3. Modificare le impostazioni relative alla voce necessarie:

   - **Consenti in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà consentito da Anti-Spam:

     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in entrata.

     - **Solo chiamate**: consente solo le chiamate in entrata.

     - **Solo SMS**: consente solo i messaggi SMS in entrata.

   - **Da numero di telefono**: numero di telefono per il quale la ricezione di messaggi SMS e/o di chiamate viene consentita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS non è spam. L'impostazione è disponibile se per l'impostazione **Consenti in entrata** è impostato il valore **Solo SMS**.

4. Premere **Indietro** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA CONSENTITI

Per eliminare una voce dalla Lista consentiti di Anti-Spam:

1. Nella scheda **Anti-Spam**, selezionare **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare dalla lista la voce da modificare e selezionare **Opzioni** → **Elimina voce**.

ELIMINAZIONE DI TUTTE LE VOCI DALLA LISTA CONSENTITI

Per eliminare tutte le voci dalla Lista consentiti di Anti-Spam:

1. Nella scheda **Anti-Spam**, selezionare **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare **Opzioni** → **Elimina tutte le voci**.

RISPOSTA AI MESSAGGI SMS E ALLE CHIAMATE DA CONTATTI NON IN RUBRICA

Se è selezionata la modalità Anti-Spam **Entrambe le liste** o **Lista consentiti** (vedere la sezione "Modalità Anti-Spam" a pagina 140), è possibile specificare una risposta di Anti-Spam verso i messaggi SMS e le chiamate provenienti da abbonati i cui numeri non sono contenuti nella rubrica. Inoltre, Anti-Spam consente di espandere la Lista consentiti aggiungendovi i numeri dall'elenco dei contatti.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per selezionare la risposta di Anti-Spam verso un numero non incluso nella rubrica:

1. Selezionare l'opzione **Modalità** nella scheda **Anti-Spam**.

   Verrà aperta la finestra **Modalità**.

2. Selezionare uno dei valori per l'impostazione **Consenti contatti** (vedere la figura sotto):

   - Per far sì che Anti-Spam consideri i numeri della rubrica come Lista consentiti aggiuntiva, selezionare il valore **Sì**;

- Per far sì che Anti-Spam filtri i messaggi SMS e le chiamate in base alla modalità Anti-Spam impostata, selezionare il valore **No**.

Figura 29. Risposta di Anti-Spam verso i numeri non inclusi nella rubrica del dispositivo

3. Premere **Indietro** per salvare le modifiche.

RISPOSTA AI MESSAGGI SMS DA MITTENTI NON NUMERICI

Se è selezionata la modalità Anti-Spam **Entrambe le liste** o **Lista bloccati** (vedere la sezione "Modalità Anti-Spam" a pagina 140), è possibile espandere ulteriormente la Lista bloccati aggiungendovi contatti non numerici (incluse le lettere). Anti-Spam bloccherà quindi i messaggi SMS provenienti dai mittenti non numerici.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per impostare la risposta di Anti-Spam alla ricezione di messaggi da mittenti non numerici:

1. Selezionare l'opzione **Modalità** nella scheda **Anti-Spam**.

   Verrà aperta la finestra **Modalità**.

2. Selezionare un valore per l'impostazione **Mittenti non numerici** (vedere la figura sotto):

   - Per far sì che Anti-Spam elimini automaticamente i messaggi SMS dai mittenti non numerici, selezionare il valore **Blocca**.

- Per far sì che Anti-Spam filtri solo i messaggi SMS da mittenti non numerici in base alla modalità Anti-Spam impostata, selezionare il valore **Consenti**.

Figura 30. Configurazione dell'azione di Anti-Spam alla ricezione di messaggi SMS da mittenti non numerici

3. Premere **Indietro** per salvare le modifiche.

SELEZIONE DI UNA RISPOSTA AI MESSAGGI SMS IN ENTRATA

Per impostazione predefinita, la modalità Anti-Spam impostata è **Entrambe le liste** (vedere la sezione "Modalità Anti-Spam" a pagina 140). Anti-Spam esegue la scansione dei messaggi SMS in entrata in base alla Lista consentiti e alla Lista bloccati.

Se il numero del mittente non è contenuto né nella Lista bloccati né nella Lista consentiti, Anti-Spam informerà l'utente e richiederà un'azione nei confronti del messaggio SMS in entrata.

È possibile selezionare una delle seguenti azioni da eseguire nei confronti del messaggio SMS (vedere la figura sotto):

- Per bloccare il messaggio SMS e aggiungere il numero di telefono del mittente alla Lista bloccati, selezionare **Opzioni → Aggiungi a Lista bloccati**.

- Per recapitare il messaggio SMS e aggiungere il numero di telefono del mittente alla Lista consentiti, selezionare **Opzioni → Aggiungi a Lista consentiti**.

- Per recapitare il messaggio SMS senza aggiungere il numero di telefono del mittente a nessuna delle liste, premere **Ignora**.

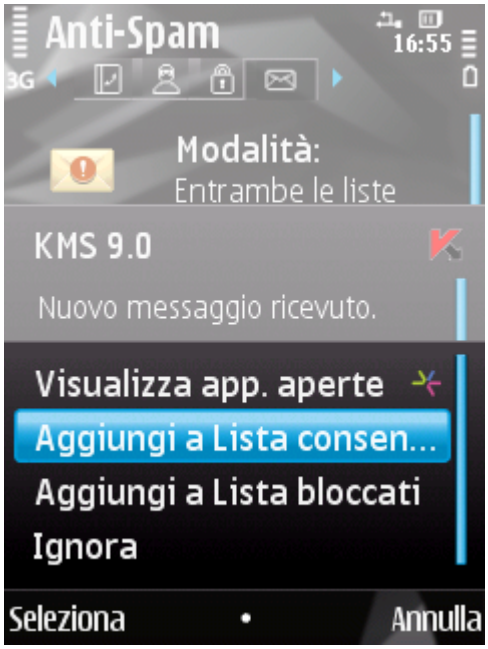


Figura 31. Notifica di Anti-Spam alla ricezione di un messaggio SMS

Le informazioni su messaggi bloccati vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

SELEZIONE DI UNA RISPOSTA ALLE CHIAMATE IN ENTRATA

Per impostazione predefinita, la modalità Anti-Spam impostata è **Entrambe le liste** (vedere la sezione "Modalità Anti-Spam" a pagina 140). Anti-Spam esegue la scansione delle chiamate in entrata in base alla Lista consentiti e alla Lista bloccati.

Se il numero del mittente non è contenuto né nella Lista bloccati né nella Lista consentiti, Anti-Spam informerà l'utente dopo aver completato la scansione e richiederà un'azione nei confronti della chiamata in entrata.

È possibile selezionare una delle seguenti azioni da eseguire per il numero da cui è stata effettuata la chiamata (vedere la figura sotto):

- Per aggiungere il numero di telefono del chiamante alla Lista bloccati, selezionare **Opzioni → Aggiungi a Lista bloccati**.

- Per aggiungere il numero di telefono del chiamante alla Lista consentiti, selezionare **Opzioni → Aggiungi a Lista consentiti**.

- **Ignora**: non aggiunge il numero del chiamante a nessuna delle liste.

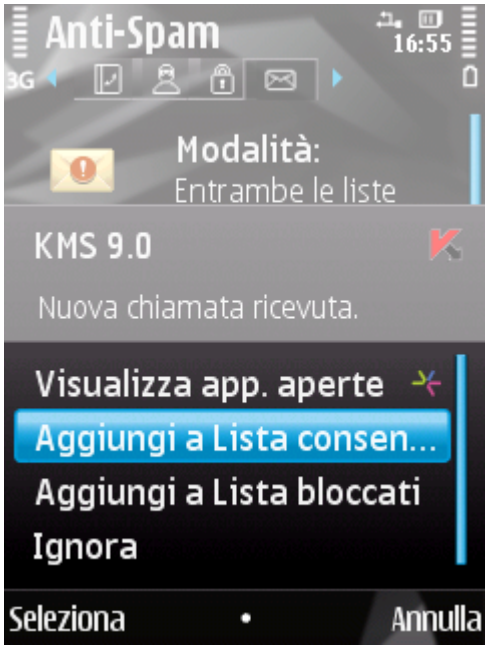


Figura 32. Notifica di Anti-Spam all'accettazione della chiamata

Le informazioni sulle chiamate bloccate vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

LIMITAZIONE DELLE CHIAMATE E DEI MESSAGGI SMS IN USCITA. PARENTAL CONTROL

Questa sezione fornisce informazioni sul componente Parental Control, che consente di limitare le chiamate e i messaggi SMS in uscita verso numeri definiti. La sezione spiega inoltre come creare una lista di numeri consentiti e bloccati e come specificare le impostazioni di Parental Control.

IN QUESTA SEZIONE

Informazioni su Parental Control 63

Modalità Parental Control 64

Modifica della modalità Parental Control 64

Creazione di una Lista bloccati 65

Creazione di una Lista consentiti 68

INFORMAZIONI SU PARENTAL CONTROL

Il componente Parental Control filtra i messaggi SMS e le chiamate in uscita utilizzando la Lista bloccati e la Lista consentiti.

Il filtro funziona nello stesso modo descritto in precedenza per il componente Anti-Spam: i messaggi SMS e le chiamate corrispondenti a una voce nella Lista bloccati vengono bloccati, mentre sono consentiti se corrispondono a una voce nella Lista consentiti.

Parental Control blocca i messaggi SMS inviati utilizzando solo le funzioni standard del dispositivo. I messaggi SMS inviati con applicazioni di terze parti non vengono bloccati.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

MODALITÀ PARENTAL CONTROL

Per modalità Parental Control si intende una configurazione di base, o una raccolta di parametri, del componente che consente a un genitore di limitare la possibilità di inviare messaggi ed effettuare chiamate indesiderate da parte di un figlio.

Sono disponibili le seguenti modalità Parental Control:

- **Disabilitato**: disabilita Parental Control. Non filtra i messaggi SMS e le chiamate in uscita.

  Questa è la modalità predefinita selezionata.

- **Lista bloccati**: blocca l'invio di messaggi SMS e/o di chiamate solo ai numeri inclusi nella Lista bloccati e consente tutti gli altri messaggi e chiamate.

- **Lista consentiti**: consente l'invio di messaggi SMS e/o di effettuare chiamate solo ai numeri inclusi nella Lista consentiti e blocca tutti gli altri messaggi e chiamate.

È possibile modificare la modalità Parental Control(vedere la sezione "Modifica della modalità Parental Control" a pagina 64).

La modalità di funzionamento corrente di Parental Control è visualizzata nella scheda **Parental Control** accanto alla voce del menu **Modalità**.

MODIFICA DELLA MODALITÀ PARENTAL CONTROL

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per modificare la modalità Parental Control:

1. Selezionare l'opzione **Modalità** nella scheda **Parental Control**.

   Verrà aperta la finestra **Modalità**.

2. Selezionare una delle modalità Parental Control suggerita (vedere la figura sotto).

Figura 33. Modifica della modalità Parental Control

3. Premere **OK** per salvare le modifiche.

CREAZIONE DI UNA LISTA BLOCCATI

È possibile creare una Lista bloccati in base alla quale Parental Control blocca i messaggi SMS e le chiamate in uscita. La lista contiene i numeri di telefono per i quali l'invio di messaggi SMS e l'effettuazione di chiamate non è bloccato.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

IN QUESTA SEZIONE

Aggiunta di voci alla Lista bloccati 65

Modifica di voci nella Lista bloccati 67

Eliminazione di voci dalla Lista bloccati 68

Eliminazione di tutte le voci dalla Lista bloccati 68

AGGIUNTA DI VOCI ALLA LISTA BLOCCATI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri di Parental Control. Se un numero è già stato salvato in una delle liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni → Cambia**.

Per aggiungere una voce alla Lista bloccati di Parental Control:

1. Selezionare **Lista bloccati** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare la voce del menu **Opzioni** → **Aggiungi voce** (vedere la figura sotto).

Figura 34. Aggiunta di voci alla Lista bloccati

3. Selezionare le seguenti impostazioni per la nuova voce (vedere la figura sotto):

   - **Blocca in uscita**: tipo di informazione in uscita da un numero di abbonato che verrà bloccato da Parental Control:

     - **Chiamate e SMS**: blocca le chiamate e i messaggi SMS in uscita.
     - **Solo chiamate**: blocca solo le chiamate in uscita.
     - **Solo SMS**: blocca solo i messaggi SMS in uscita.

- **Numero di telefono**: numero di telefono bloccato per i messaggi SMS e/o le chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

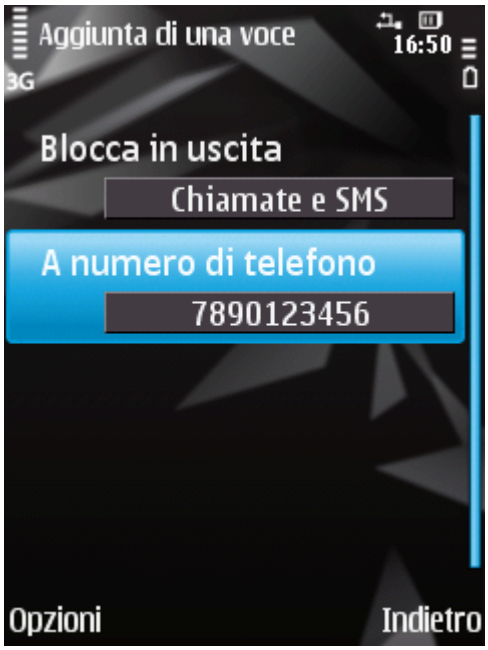


Figura 35. Impostazioni della voce

4. Premere **Indietro** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA BLOCCATI

È possibile cambiare il valore di tutte le impostazioni relative ai numeri presenti nella Lista bloccati.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni → Cambia**.

Per modificare una voce della Lista bloccati di Parental Control:

1. Selezionare **Lista bloccati** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare dalla lista la voce che si desidera modificare e selezionare **Opzioni → Modifica voce**.

3. Modificare le impostazioni relative alla voce necessarie:

   - **Blocca in uscita**: tipo di informazione in uscita da un numero di abbonato che verrà bloccato da Parental Control:

     - **Chiamate e SMS**: blocca le chiamate e i messaggi SMS in uscita.

     - **Solo chiamate**: blocca solo le chiamate in uscita.

     - **Solo SMS**: blocca solo i messaggi SMS in uscita.

   - **Numero di telefono**: numero di telefono bloccato per i messaggi SMS e/o le chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

4. Premere **Indietro** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA BLOCCATI

In caso di aggiunta accidentale di un numero alla Lista bloccati è possibile eliminare tale numero dalla lista.

Per eliminare una voce dalla Lista bloccati di Parental Control, eseguire le seguenti operazioni:

1. Selezionare **Lista bloccati** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare dalla lista la voce da modificare e selezionare **Opzioni** → **Elimina voce**.

ELIMINAZIONE DI TUTTE LE VOCI DALLA LISTA BLOCCATI

Per eliminare tutte le voci dalla Lista bloccati di Parental Control:

1. Selezionare **Lista bloccati** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista bloccati**.

2. Selezionare **Opzioni** → **Elimina tutte le voci**.

La lista verrà svuotata.

CREAZIONE DI UNA LISTA CONSENTITI

È possibile creare una Lista consentiti in base alla quale Parental Control consente l'invio di messaggi SMS e l'effettuazione di chiamate.

La lista contiene i numeri di telefono per i quali Parental Control consente l'invio di messaggi SMS e l'effettuazione di chiamate.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

IN QUESTA SEZIONE

Aggiunta di voci 68

Modifica di voci nella Lista consentiti 70

Eliminazione di voci dalla Lista consentiti 71

Eliminazione di tutte le voci 71

AGGIUNTA DI VOCI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri di Parental Control. Se un numero è già stato salvato in una delle liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni → Cambia**.

Per aggiungere una voce alla Lista consentiti di Parental Control:

1. Selezionare **Lista consentiti** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare **Opzioni → Aggiungi voce** (vedere la figura sotto).

Figura 36. Aggiunta di voci alla Lista consentiti

3. Selezionare le seguenti impostazioni per la nuova voce (vedere la figura sotto):

   - **Consenti in uscita**: tipo di informazione in uscita che Parental Control consente di inviare a un numero di abbonato:
     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in uscita.
     - **Solo chiamate**: consente solo le chiamate in uscita.
     - **Solo SMS**: consente solo i messaggi SMS in uscita.

- **Numero di telefono**: numero di telefono al quale i messaggi SMS e/o le chiamate in uscita sono consentite da Parental Control. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

Figura 37. Impostazioni della voce

4. Premere **Indietro** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA CONSENTITI

È possibile cambiare i valori di tutte le impostazioni relative ai numeri presenti nella Lista consentiti.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per modificare una voce della Lista consentiti di Parental Control:

1. Selezionare **Lista consentiti** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare dalla lista la voce che si desidera modificare e selezionare **Opzioni** → **Modifica voce**.

3. Modificare le impostazioni relative alla voce necessarie:

   - **Consenti in uscita**: tipo di informazione in uscita che Parental Control consente di inviare a un numero di abbonato:
     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in uscita.
     - **Solo chiamate**: consente solo le chiamate in uscita.
     - **Solo SMS**: consente solo i messaggi SMS in uscita.
   - **Numero di telefono**: numero di telefono al quale i messaggi SMS e/o le chiamate in uscita sono consentite da Parental Control. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

4. Premere **Indietro** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA CONSENTITI

In caso di aggiunta accidentale di un numero alla Lista consentiti è possibile eliminare tale numero dalla lista creata.

Per eliminare una voce dalla Lista consentiti di Parental Control:

1. Selezionare **Lista consentiti** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare dalla lista la voce da modificare e selezionare **Opzioni → Elimina voce**.

ELIMINAZIONE DI TUTTE LE VOCI

Per eliminare tutte le voci dalla Lista consentiti di Parental Control:

1. Selezionare **Lista consentiti** nella scheda **Parental Control**.

   Verrà aperta la finestra **Lista consentiti**.

2. Selezionare **Opzioni→ Elimina tutte le voci**.

La lista verrà svuotata.

PROTEZIONE DEI DATI IN CASO DI SMARRIMENTO O FURTO DEL DISPOSITIVO

Questa sezione fornisce informazioni sul componente Antifurto che assicura una protezione elevatadei dati personali in caso di furto o smarrimento del dispositivo e facilita la ricerca del dispositivo stesso. La sezione spiega inoltre come abilitare/disabilitare la funzione Antifurto, come impostare i parametri di funzionamento e come avviare la protezione in remoto in caso di furto o smarrimento del dispositivo.

IN QUESTA SEZIONE

Informazioni su Antifurto 72

Blocco del dispositivo 72

Eliminazione dei dati personali 74

Creazione di un elenco di oggetti da eliminare 76

Monitoraggio della sostituzione di una scheda SIM sul dispositivo 77

Determinazione delle coordinate geografiche del dispositivo 78

Avvio da remoto delle funzioni di Antifurto 80

INFORMAZIONI SU ANTIFURTO

Il componente Antifurto protegge i dati memorizzati nel dispositivo da accessi non autorizzati. Questa funzione può essere utile in caso di smarrimento o furto del dispositivo. Antifurto consente il blocco da remoto del dispositivo e la cancellazione dei dati memorizzati su di esso.

Questo componente comprende le seguenti funzioni:

- **SMS-Block**: consente di bloccare il dispositivo su richiesta dell'utente e di specificare un testo da visualizzare sullo schermo in modalità blocco.
- **SMS-Clean**: consente di cancellare in modo irreversibile dal dispositivo i dati personali dell'utente (tutti i contatti, messaggi, galleria, calendario, registri e impostazioni di accesso alla rete), i dati contenuti nelle schede di memoria e i file presenti nelle cartelle selezionate.
- **SIM Watch**: avvisa l'utente e blocca il dispositivo derubato se viene sostituita la scheda SIM o se il dispositivo viene acceso senza la scheda SIM. La funzione SIM Watch invia un messaggio contenente il nuovo numero di telefono del dispositivo a un numero di telefono specificato e/o a un indirizzo e-mail.
- **SMS-Find**: consente all'utente di determinare da remoto la posizione del dispositivo, che può essere inviata tramite messaggio al dispositivo richiedente o a un indirizzo e-mail specificato.

  Questa opzione funziona solo su dispositivi con ricevitore GPS integrato.

Per poter utilizzare tutte le funzioni di Antifurto, è necessario ricordare la password segreta creata alla prima esecuzione di Kaspersky Mobile Security 9.0.

Dopo l'installazione di Kaspersky Mobile Security 9.0, tutte le funzioni di Antifurto sono disabilitate.

Inoltre, Kaspersky Mobile Security 9.0 consente di avviare da remoto la funzione Antifurto inviando un comando al dispositivo smarrito o derubato (vedere la sezione "Avvio remoto delle funzioni Antifurto" a pagina 80).

Lo stato corrente di ogni funzione viene visualizzato nella scheda **Antifurto** accanto al nome della funzione.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

BLOCCO DEL DISPOSITIVO

In caso di smarrimento o furto del dispositivo, la funzione SMS-Block consente il blocco da remoto dell'accesso al dispositivo e ai dati memorizzati su di esso. Il dispositivo può essere sbloccato solo dopo aver immesso la password segreta.

Questa funzione non blocca il dispositivo ma abilita semplicemente l'opzione di blocco remoto.

Per modificare le impostazioni, utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per abilitare la funzione SMS-Block:

1. Selezionare l'opzione **SMS-Block** nella scheda **Antifurto**.

   Verrà aperta la finestra **SMS-Block**.

2. Selezionare il valore **Abilitato** per l'impostazione **Modalità SMS-Block**.

3. Per visualizzare il testo sullo schermo di un dispositivo bloccato, selezionare l'opzione **Testo quando bloccato** e compilare il campo **Immettere testo** (vedere la figura sotto). Quando il dispositivo è bloccato, per impostazione predefinita sullo schermo viene visualizzato il testo Dispositivo bloccato.

   Per evitare la visualizzazione del testo, selezionare l'impostazione **Testo quando bloccato**, eliminare il contenuto del campo **Immettere testo** e premere **OK**.

Figura 38. Impostazioni della funzione SMS-Block

4. Premere **Indietro** per salvare le modifiche.

Se la funzione SMS-Block è abilitata, è possibile bloccare il dispositivo utilizzando i seguenti metodi:

- Utilizzando il comando Invia. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo da bloccare. La ricezione del messaggio SMS speciale sul dispositivo bloccato è invisibile all'utente.

- Utilizzando un telefono per inviare un messaggio SMS standard. Per eseguire questa operazione, è necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo da bloccare.

Per inviare un comando al dispositivo smarrito:

1. Nella scheda **Avanzate**, selezionare **Invia comando**.

   Verrà aperta una finestra di invio del comando speciale.

2. Premere **Avvio**.

3. Selezionare il tipo di comando **SMS-Block** e premere **Avanti** (vedere la figura sotto).

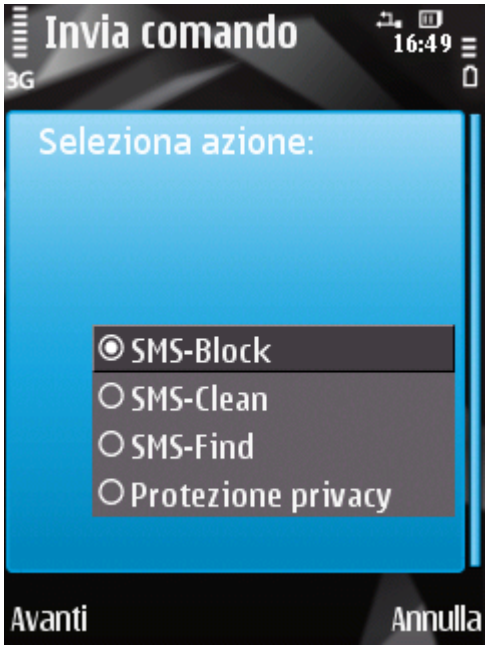


Figura 39. Blocco remoto del dispositivo

4. Immettere il numero di telefono del dispositivo da bloccare e premere **Avanti**.

5. Immettere la password segreta specificata sul dispositivo che riceverà il messaggio e premere **Invia**.

Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

inviare un messaggio SMS standard al dispositivo che si desidera bloccare. Il messaggio SMS deve contenere il testo `block:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

ELIMINAZIONE DEI DATI PERSONALI

In caso di furto o smarrimento del dispositivo mobile, la funzione SMS-Clean consente la cancellazione remota delle seguenti informazioni memorizzate sul dispositivo:

- dati personali dell'utente (tutti i contatti, messaggi, galleria, calendario e impostazioni di connessione alla rete), mentre Antifurto elimina i contatti memorizzati nella rubrica e sulla scheda SIM;
- dati contenuti nelle schede di memoria;
- file presenti nella cartella C:\Data e in altre cartelle specificate.

Questa funzione non elimina i dati memorizzati sul dispositivo, ma include l'opzione di cancellazione.

Antifurto eliminerà i dati dall'elenco di oggetti da eliminare creato solo dopo che il dispositivo ha ricevuto il messaggio SMS speciale (vedere la sezione "Creazione di un elenco di oggetti da eliminare" a pagina 76).

Per abilitare la funzione SMS-Clean:

1. Nella scheda **Antifurto**, selezionare **SMS-Clean**.

   Verrà aperta la finestra **SMS-Clean**.

2. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **Modalità**.

3. Selezionare l'opzione **Modalita SMS-Clean** e impostare il valore **Abilitato** (vedere la figura sotto).

4. Selezionare i dati da cancellare quando il dispositivo riceve uno speciale messaggio SMS:

   - per cancellare i dati personali, per l'impostazione **Elimina dati** selezionare il valore **Sì**;
   - per cancellare i file da C:\Data e da altre cartelle specificate, per l'impostazione **Elimina cartelle**, selezionare **Sì**.

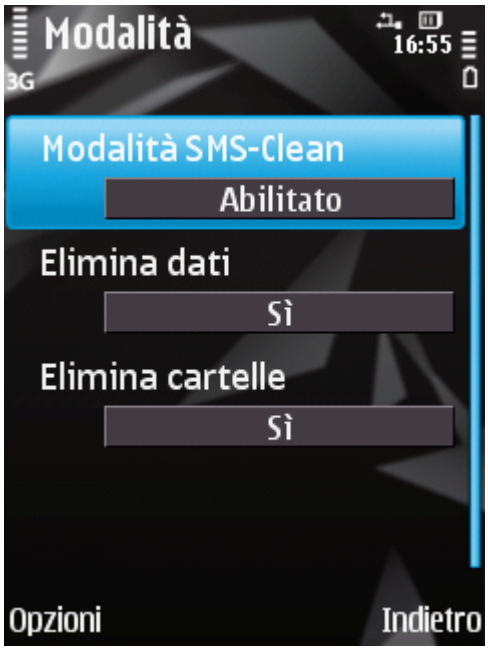


Figura 40. Impostazioni della funzione SMS-Clean

5. Premere **Indietro** per salvare le modifiche.

6. Passare alla creazione di un elenco di cartelle da eliminare (vedere la sezione "Creazione di un elenco di oggetti da eliminare" a pagina 76).

Abilitando la funzione, è possibile eliminare dal dispositivo i dati personali utilizzando i seguenti metodi:

- Inviando un comando al dispositivo smarrito o derubato. Utilizzando il comando Invia. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo. La ricezione del messaggio SMS speciale sul dispositivo derubato o smarrito è invisibile all'utente.

- Utilizzando un telefono per inviare un messaggio SMS standard. È necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo smarrito o derubato.

➧ *Per inviare un comando al dispositivo smarrito o derubato:*

1. Nella scheda **Avanzate**, selezionare **Invia comando**.

   Verrà aperta una finestra di invio del comando speciale.

2. Premere **Avvio**.

3. Selezionare il tipo di comando **SMS-Clean** e premere **Avanti** (vedere la figura sotto).

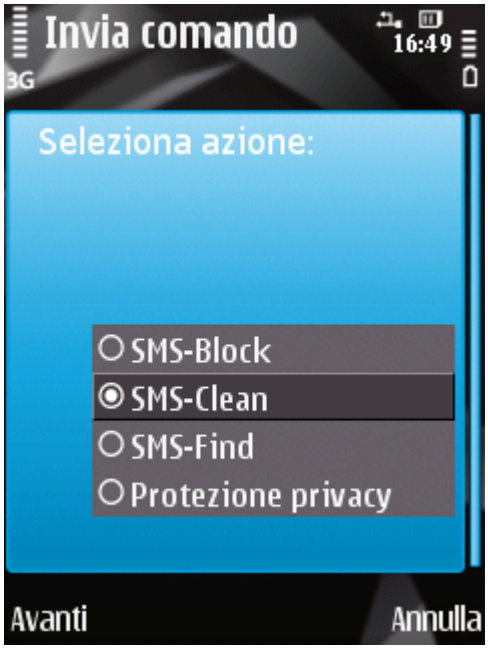


Figura 41. Eliminazione dei dati personali

4. Immettere il numero di telefono del dispositivo su cui devono essere eliminati i dati e premere **Avanti**.

5. Immettere la password segreta specificata sul dispositivo che riceverà il messaggio e premere **Invia**.

➧ *Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,*

inviare un messaggio SMS al dispositivo smarrito o derubato. Il messaggio SMS deve contenere il testo `wipe:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

CREAZIONE DI UN ELENCO DI OGGETTI DA ELIMINARE

➧ *Per aggiungere una cartella all'elenco di cartelle da eliminare:*

1. Nella scheda **Antifurto**, selezionare **SMS-Clean**.

   Verrà aperta la finestra **SMS-Clean**.

2. Selezionare l'opzione **Cartelle da eliminare** .

   Verrà aperta la finestra **Cartelle da eliminare**.

3. Selezionare **Opzioni** → **Aggiungi cartella** (vedere la figura sotto).

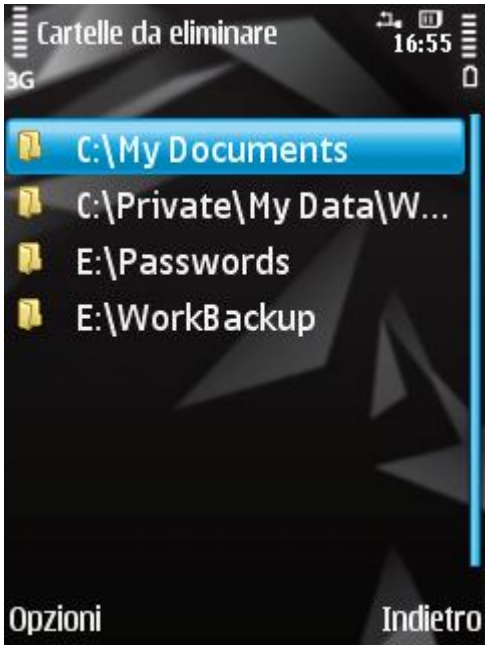


Figura 42. Aggiunta di cartelle

4. Selezionare la cartella desiderata dalla struttura di cartelle e premere**OK**.

   La cartella verrà aggiunta all'elenco.

5. Premere **Indietro** per salvare le modifiche.

- *Per rimuovere una cartella dall'elenco:*

1. Nella scheda **Antifurto**, selezionare **SMS-Clean**.

   Verrà aperta la finestra **SMS-Clean**.

2. Selezionare l'opzione **Cartelle da eliminare** .

   Verrà aperta la finestra **Cartelle da eliminare**.

3. Selezionare una cartella dall'elenco e selezionare **Opzioni** → **Elimina cartella**.

4. Confermare la disinstallazione premendo il pulsante **Sì**.

MONITORAGGIO DELLA SOSTITUZIONE DI UNA SCHEDA SIM SUL DISPOSITIVO

La funzione SIM Watch invia un messaggio contenente il nuovo numero della scheda SIM inserita a un numero di telefono e/o all'indirizzo e-mail specificato e blocca il dispositivo in caso di sostituzione della scheda SIM sul dispositivo smarrito o derubato.

- *Per abilitare la funzione SIM Watch e controllare la sostituzione della scheda SIM:*

1. Selezionare l'opzione **SIM Watch** nella scheda **Antifurto**.

   Verrà aperta la finestra **SIM Watch**.

2. Selezionare l'opzione **Modalità SIM Watch** e impostare il valore **Abilitato**.

3. Configurare le seguenti impostazioni di SIM Watch (vedere la figura sotto):

   - **Indirizzo e-mail**. Per ricevere un messaggio e-mail con il nuovo numero del proprio telefono, immettere un indirizzo e-mail.

   - **Numero di telefono**. Per inviare automaticamente un messaggio con il nuovo numero del proprio telefono, immettere il numero di telefono al quale deve essere inviato il messaggio. Il numero di telefono può iniziare con una cifra o con un "+" e deve contenere solo cifre.

   - **Se scheda SIM sostituita**. Per bloccare il dispositivo se la scheda SIM viene sostituita o se il dispositivo viene acceso senza di essa, impostare il valore **Blocca**. È possibile sbloccare il dispositivo solo dopo aver immesso la password segreta. Per impostazione predefinita, il blocco del dispositivo è disabilitato.

   - **Testo quando bloccato**. Per visualizzare un messaggio sullo schermo in modalità blocco, inserirlo nel campo **Immettere testo**. Per impostazione predefinita, viene inserito il testo Dispositivo bloccato.

Figura 43. Impostazioni della funzione SIM Watch

4. Premere **Indietro** per salvare le modifiche.

DETERMINAZIONE DELLE COORDINATE GEOGRAFICHE DEL DISPOSITIVO

La funzione SMS-Find è in grado di inviare le coordinate geografiche del dispositivo a un dispositivo richiedente mediante un messaggio SMS e/o a un indirizzo e-mail specificato.

Questa opzione funziona solo su dispositivi con ricevitore GPS integrato. Se necessario, il ricevitore sarà attivato automaticamente.

Le coordinate possono essere ottenute solo se il dispositivo si trova in un'area coperta da satelliti. Se non sono disponibili satelliti al momento della richiesta, verranno effettuati dei tentativi di ricerca ad intervalli specifici.

Per abilitare la funzione SMS-Find:

1. Selezionare l'opzione **SMS-Find** nella scheda **Antifurto**.

   Verrà aperta la finestra **SMS-Find**.

2. Selezionare il valore **Abilitato** per l'impostazione **Modalità SMS-Find**.

3. Immettere per l'impostazione **Indirizzo e-mail** l'indirizzo e-mail cui devono essere inviate le coordinate del dispositivo (vedere la figura sotto).

Figura 44. Impostazioni della funzione SMS-Find

4. Premere **Indietro** per salvare le modifiche.

È possibile richiedere le coordinate di un dispositivo su cui è abilitata la funzione SMS-Find utilizzando i seguenti metodi:

- Utilizzando il comando Invia. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo. La ricezione del messaggio SMS speciale sul dispositivo derubato o smarrito è invisibile all'utente.

- Opzioni standard di creazione dei messaggi SMS sul telefono. È necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo smarrito o derubato.

Per inviare un comando al dispositivo smarrito o derubato:

1. Nella scheda **Avanzate**, selezionare **Invia comando**.

   Verrà aperta una finestra di invio del comando speciale.

2. Selezionare il tipo di comando **SMS-Find** e premere **Avanti** (vedere la figura sotto).

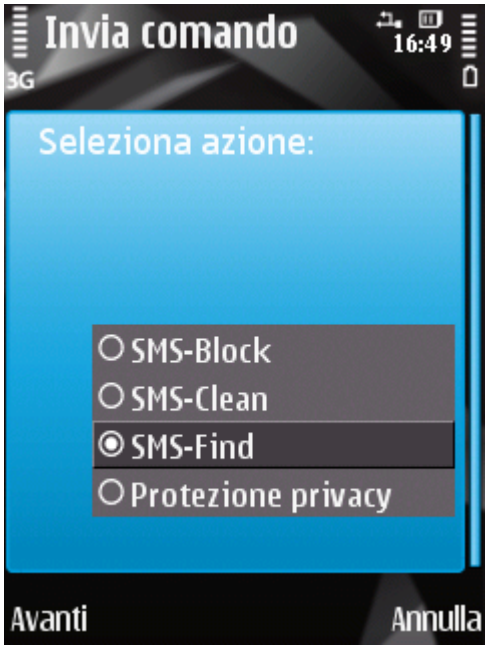


Figura 45. Determinazione della posizione del dispositivo

3. Immettere il numero di telefono del dispositivo di cui si desidera ricevere le coordinate e premere **Avanti**.

4. Immettere la password segreta specificata sul dispositivo che riceverà il messaggio e premere **Invia**.

Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

inviare un messaggio SMS al dispositivo smarrito o derubato. Il messaggio SMS deve contenere il testo `find:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

Verrà inviato un messaggio SMS con le coordinate del dispositivo al numero da cui è stata inviata la richiesta di ricevere le coordinate e all'indirizzo e-mail, se specificato nelle impostazioni SMS-Find.

AVVIO REMOTO DELLE FUNZIONI DI ANTIFURTO

È possibile inviare un comando con uno speciale messaggio SMS per avviare da remoto la funzione Antifurto sul dispositivo smarrito o derubato su cui è installato Kaspersky Mobile Security. Il comando viene ricevuto sul dispositivo bloccato in modo invisibile all'utente.

Per inviare un comando al dispositivo smarrito o derubato:

1. Nella scheda **Avanzate**, selezionare **Invia comando**.

   Verrà aperta una finestra di invio del comando speciale.

2. Premere **Avvio**.

3. Selezionare una delle funzioni suggerite da avviare in remoto (vedere la figura sotto):

   - **SMS-Block** (vedere la sezione "Blocco del dispositivo" a pagina 72).
   - **SMS-Clean** (vedere la sezione "Eliminazione dei dati personali" a pagina 74).

- **SMS-Find** (vedere la sezione "Determinazione delle coordinate geografiche del dispositivo" a pagina 78).
- **Protezione privacy** (vedere la sezione "Protezione privacy" a pagina 82).

Figura 46. Avvio remoto delle funzioni di Antifurto

La funzione utilizzata deve essere abilitata sul dispositivo che riceverà il messaggio.

4. Premere **Avanti**.
5. Immettere il numero di telefono al quale verrà inviato il messaggio e premere **Avanti**.
6. Immettere la password segreta specificata sul dispositivo che riceverà il messaggio e premere **Invia**.

MASCHERAMENTO DEI DATI PERSONALI

Questa sezione fornisce informazioni su Protezione privacy. Il componente abilita il mascheramento dei dati riservati dell'utente mentre il dispositivo viene utilizzato temporaneamente da un'altra persona.

IN QUESTA SEZIONE

Protezione privacy 82
Modalità di Protezione privacy 82
Modifica della modalità di Protezione privacy 82
Avvio automatico di Protezione privacy 83
Avvio remoto di Protezione privacy 84
Creazione di un elenco di contatti protetti 86
Selezione degli oggetti di protezione: Protezione privacy 88

PROTEZIONE PRIVACY

Il componente Protezione privacy protegge i dati personali dell'utente e impedisce l'accesso indesiderato alle informazioni personali mentre altre persone utilizzano temporaneamente il dispositivo. Il componente abilita il mascheramento dei dati riservati dell'utente, come i contatti (salvati nella memoria del dispositivo, sulla scheda SIM o su un supporto rimovibile), i messaggi e le chiamate.

Il componente Protezione privacy analizza i dati in base a un elenco di contatti protetti (vedere la sezione "Selezione degli oggetti di protezione: Protezione privacy" a pagina 88). Il componente nasconde le seguenti informazioni relative ai numeri di questo elenco:

- informazioni nell'elenco contatti;
- voce del numero nel registro chiamate (in entrata, in uscita, perse).
- messaggi SMS nell'elenco dei messaggi SMS in entrata, in uscita, eliminati e inviati.

Le informazioni sul funzionamento di Protezione privacy vengono memorizzate nel report (vedere "Report dell'applicazione" a pagina 102).

MODALITÀ DI PROTEZIONE PRIVACY

Kaspersky Mobile Security 9.0 consente di gestire la protezione dei dati personali dell'utente. Il componente Protezione privacy viene avviato manualmente. Per impostazione predefinita, è disabilitato.

Protezione privacy può funzionare in una delle seguenti modalità:

- **Normale**: la protezione dei dati riservati è disabilitata. Le impostazioni di Protezione privacy sono accessibili per la modifica.
- **Privato**: la protezione dei dati riservati è abilitata. Il componente Protezione privacy nasconde tutti i dati relativi ai contatti protetti. Le impostazioni di Protezione privacy non possono essere modificate.

La modalità di funzionamento corrente del componente è visualizzata nella scheda **Protezione privacy** accanto alla voce del menu **Modalità**.

La modifica della modalità di Protezione privacy può richiedere un certo tempo.

MODIFICA DELLA MODALITÀ DI PROTEZIONE PRIVACY

La modalità di Protezione privacy può essere modificata come indicato di seguito:

- dall'interfaccia dell'applicazione;
- tramite la password segreta quando il dispositivo è in standby.

Per modificare la modalità di Protezione privacy:

1. Selezionare l'opzione **Modalità** nella scheda **Protezione privacy**.

   Verrà aperta la finestra **Modalità Privacy**.

2. Selezionare un valore per l'impostazione **Modalità Privacy** (vedere la figura sotto).

Figura 47. Modifica della modalità di Protezione privacy

3. Premere **Indietro** per salvare le modifiche.

Per modificare la modalità di Protezione privacy tramite la password segreta quando il dispositivo è in standby,

immettere il comando ***secret code#**.

Quando si modifica la modalità di Protezione privacy, sullo schermo del dispositivo apparirà un notifica.

AVVIO AUTOMATICO DI PROTEZIONE PRIVACY

La protezione dei dati riservati viene avviata per impostazione predefinita immediatamente dopo l'abilitazione di Protezione privacy.

È possibile impostare un tempo allo scadere del quale il componente Protezione privacy verrà avviato automaticamente.

Disabilitare Protezione privacy prima di modificare le sue impostazioni.

Per configurare l'avvio automatico di Protezione privacy alla scadenza di un tempo specificato:

1. Selezionare l'opzione **Modalità** nella scheda **Protezione privacy**.

   Verrà aperta la finestra **Modalità Privacy**.

2. Selezionare un tempo allo scadere del quale il componente Protezione privacy verrà abilitato automaticamente. Per eseguire questa operazione, impostare uno dei valori suggeriti per l'impostazione **Nascondi autom.** (vedere la figura sotto).

   - **Nessun ritardo**.
   - **Dopo 1 minuto**.
   - **Dopo 5 minuti**.

- **Dopo 15 minuti**.
- **Dopo 1 ora**.
- **Disabilitato**.

Figura 48. Avvio automatico di Protezione privacy

3. Premere **Indietro** per salvare le modifiche.

AVVIO REMOTO DI PROTEZIONE PRIVACY

Kaspersky Mobile Security 9.0 consente di avviare da remoto Protezione privacy tramite uno speciale messaggio SMS. Per eseguire questa operazione, abilitare prima la funzione che consente l'avvio remoto di Protezione privacy.

Per consentire l'avvio remoto di Protezione privacy:

1. Selezionare l'opzione **Modalità** nella scheda **Protezione privacy**.

   Verrà aperta la finestra **Modalità Privacy**.

2. Selezionare il valore **Sì** per l'impostazione **Nascondi su SMS** (vedere la figura sotto).

Figura 49. Impostazioni di abilitazione remota di Protezione privacy

3. Premere **Indietro** per salvare le modifiche.

Il componente Protezione privacy può essere avviato da remoto come indicato di seguito:

- Inviando un comando al dispositivo smarrito o derubato. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo. La ricezione del messaggio SMS speciale sul dispositivo derubato o smarrito è invisibile all'utente.

- Opzioni standard di creazione dei messaggi SMS sul telefono. È necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo smarrito o derubato.

Per inviare un comando al dispositivo smarrito o derubato:

1. Nella scheda **Avanzate**, selezionare **Invia comando**.

   Verrà aperta una finestra di invio del comando speciale.

2. Premere **Avvio**.

3. Selezionare il tipo di comando **Protezione privacy** e premere **Avanti** (vedere la figura sotto).

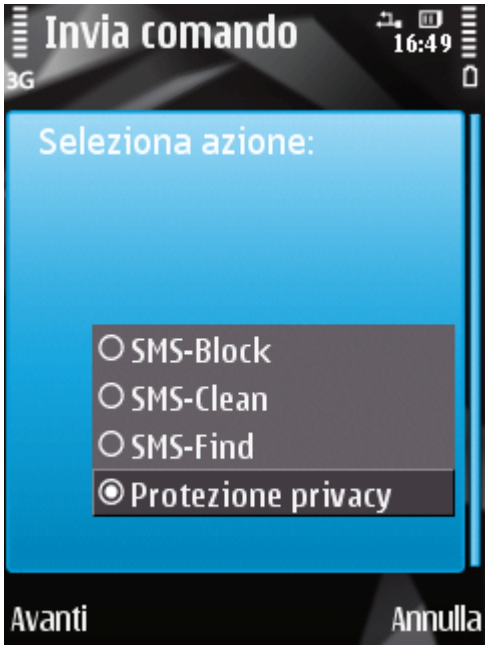


Figura 50. Avvio remoto di Protezione privacy

4. Immettere il numero di telefono del dispositivo su cui devono essere nascosti i dati e premere **Avanti**.

5. Immettere la password segreta specificata sul dispositivo che riceverà il messaggio e premere **Invia**.

Alla ricezione del comando, il componente Protezione privacy viene avviato automaticamente sul dispositivo smarrito o derubato.

Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

inviare un messaggio SMS standard al dispositivo che si desidera rintracciare. Il messaggio SMS deve contenere il testo `hide:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo ricevente. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

CREAZIONE DI UN ELENCO DI CONTATTI PROTETTI

Il componente Protezione privacy nasconde i dati personali (ad esempio, i messaggi SMS e le chiamate) collegati a determinati abbonati. I numeri degli abbonati vengono salvati nell'elenco dei contatti protetti.

IN QUESTA SEZIONE

Aggiunta di un numero all'elenco dei contatti protetti 86

Modifica di un numero nell'elenco dei contatti protetti 87

Eliminazione di un numero dall'elenco dei contatti protetti 88

AGGIUNTA DI UN NUMERO ALL'ELENCO DEI CONTATTI PROTETTI

È possibile aggiungere all'elenco dei contatti protetti qualunque numero di telefono e nome di contatto salvato sulla scheda SIM o nella rubrica del dispositivo.

Disabilitare Protezione privacy prima di modificare le sue impostazioni.

Per modificare una voce nell'elenco dei contatti protetti:

1. Selezionare l'opzione **Elenco contatti** nella scheda **Protezione privacy**.

   Verrà aperta la finestra **Elenco contatti**.

2. Eseguire una delle seguenti operazioni (vedere la figura sotto):

   - Per aggiungere un numero, selezionare **Opzioni→ Aggiungi voce→ Numero**. Nella finestra **Numero** visualizzata, compilare il campo **Immetti numero telef.**. Al completamento dell'operazione, premere **OK**.

   - Per aggiungere un numero dalla rubrica, selezionare **Opzioni → Aggiungi voce → Contatti**. Quindi, nella finestra **Contatti** visualizzata, selezionare il contatto desiderato dalla rubrica utilizzando il menu **Opzioni → Seleziona**. Al completamento dell'operazione, premere **OK**.

   - Per aggiungere un numero salvato sulla scheda SIM, selezionare **Opzioni → Aggiungi voce →Contatto da SIM**. Quindi, nella finestra **Contatti** visualizzata, selezionare il contatto desiderato sulla scheda SIM utilizzando il menu **Opzioni → Seleziona**. Al completamento dell'operazione, premere **OK**.

Figura 51. Aggiunta di voci all'elenco dei contatti protetti

3. Premere **Indietro** per salvare le modifiche.

MODIFICA DI UN NUMERO NELL'ELENCO DEI CONTATTI PROTETTI

È possibile modificare solo i numeri di telefono immessi manualmente. Non è possibile modificare i numeri selezionati dalla rubrica o da un elenco di numeri sulla scheda SIM.

Disabilitare il componente Protezione privacy prima di modificare le sue impostazioni.

Per modificare un numero di telefono nell'elenco dei contatti protetti:

1. Selezionare l'opzione **Protezione privacy** nella scheda **Elenco contatti**.

Verrà aperta la finestra **Elenco contatti**.

2. Selezionare dalla lista il numero che si desidera modificare e selezionare **Opzioni → Modifica voce**.

   Sullo schermo apparirà il numero di telefono del contatto selezionato.

3. Modificare i dati nel campo **Immettere numero di telefono**.

4. Al termine della modifica, premere **OK**.

ELIMINAZIONE DI UN NUMERO DALL'ELENCO DEI CONTATTI PROTETTI

È possibile eliminare uno o tutti i numeri dall'elenco dei contatti protetti.

- *Per eliminare un numero:*

  1. Selezionare l'opzione **Elenco contatti** nella scheda **Protezione privacy**.

     Verrà aperta la finestra **Elenco contatti**.

  2. Selezionare un elemento dalla lista e selezionare **Opzioni → Elimina voce**.

  3. Confermare l'eliminazione premendo **Sì**.

- *Per svuotare l'elenco dei contatti protetti:*

  1. Selezionare l'opzione **Elenco contatti** nella scheda **Protezione privacy**.

     Verrà aperta la finestra **Elenco contatti**.

  2. Selezionare **Opzioni → Elimina tutte le voci**.

  3. Confermare l'eliminazione premendo **Sì**.

L'elenco dei contatti protetti verrà svuotato.

SELEZIONE DEGLI OGGETTI DI PROTEZIONE: PROTEZIONE PRIVACY

Quando il componente Protezione privacy è abilitato, i contatti, i messaggi e le voci nei registri chiamate relativi ai contatti protetti sono nascosti per impostazione predefinita. È possibile selezionare i dati il cui accesso è limitato.

Disabilitare Protezione privacy prima di modificare le sue impostazioni.

- *Per selezionare gli oggetti di protezione per i numeri protetti:*

  1. Nella scheda **Protezione privacy**, selezionare l'opzione **Nascondi protezione**.

     Verrà aperta la finestra **Oggetti nascosti**.

  2. Selezionare gli oggetti da nascondere per i numeri protetti. Per ogni impostazione necessaria, impostare il valore **Nascondi** utilizzando il menu **Opzioni → Cambia**. Sarà disponibile l'opzione per nascondere i seguenti oggetti (vedere la figura sotto):

     - **Contatti**: nasconde nella rubrica del dispositivo tutti i dati sui numeri protetti.
     - **Messaggi**: nasconde nell'elenco dei messaggi SMS in entrata/uscita tutti gli SMS dai numeri protetti.
     - **Voci chiamata**: accetta le chiamate dai numeri protetti, ma nasconde il numero del chiamante e non visualizza le informazioni sui numeri protetti nell'elenco delle chiamate (in entrata, in uscita, perse).

- **Chiamate in entrata**: blocca le chiamate dai numeri dell'Elenco contatti (in questo caso il chiamante udirà il segnale di occupato). Le informazioni sulla chiamata ricevuta vengono visualizzate solo se il componente Protezione privacy è disabilitato.

- **SMS in entrata**: non visualizza il recapito dei messaggi SMS in entrata (sullo schermo non verrà visualizzato alcun messaggio sulla ricezione di un nuovo messaggio SMS da un numero nascosto). Tutti i messaggi SMS ricevuti dai numeri nascosti possono essere visualizzati se il componente Protezione privacy è disabilitato.

Figura 52. Selezione di oggetti nascosti

3. Premere **Indietro** per salvare le modifiche.

FILTRO DELL'ATTIVITÀ DI RETE. FIREWALL

Questa sezione fornisce informazioni sul componente Firewall che monitorizza le connessioni in entrata e in uscita sul dispositivo. La sezione spiega inoltre come abilitare/disabilitare il funzionamento del componente e come selezionare il livello di sicurezza richiesto.

IN QUESTA SEZIONE

Informazioni su Firewall 89

Livelli di sicurezza di Firewall 90

Selezione del livello di sicurezza di Firewall 90

Notifica del tentativo di connessione 91

INFORMAZIONI SU FIREWALL

La funzione Firewall analizza tutte le connessioni di rete sul dispositivo bloccando o consentendo l'attività di rete in base al livello di sicurezza selezionato.

Al termine dell'installazione, il componente Firewall di Kaspersky Mobile Security 9.0 è disabilitato.

Per conoscere tutte le connessioni bloccate, utilizzare la notifica Firewall (vedere la sezione "Notifica del tentativo di connessione" a pagina 91).

Le informazioni sul funzionamento di Firewall vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

LIVELLI DI SICUREZZA DI FIREWALL

Il funzionamento di Firewall è basato su livelli di sicurezza. Il livello di sicurezza determina quali protocolli di rete possono essere utilizzati per trasferire le informazioni e quali di essi sono bloccati.

Sono disponibili i seguenti livelli di sicurezza:

- **Disabilitato**: tutte le attività di rete sono consentite. Questo è il livello di sicurezza predefinito selezionato.
- **Sono bloccate solo le connessioni in entrata.**: blocca solo le connessioni in entrata. Le connessioni in uscita sono consentite.
- **Sono ammesse le connessioni in uscita mediante i protocolli SSH, HTTP, HTTPS, IMAP, SMTP e POP3**: blocca tutte le connessioni in entrata Sono accessibili il controllo delle e-mail, la visualizzazione di siti web e il download di file. Le connessioni in uscita possono essere stabilite solo mediate le porte SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Blocca tutto**: blocca tutte le attività di rete tranne l'aggiornamento del database dell'applicazione e il rinnovo della licenza.

È possibile cambiare il livello di sicurezza di Firewall (vedere la sezione "Selezione del livello di sicurezza di Firewall" a pagina 90). La modalità corrente è visualizzata nella scheda Firewall accanto alla voce del menu **Modalità**.

SELEZIONE DEL LIVELLO DI SICUREZZA DI FIREWALL

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per impostare il livello di sicurezza di Firewall:

1. Selezionare l'opzione **Modalità** nella scheda **Firewall**.

   Verrà aperta la finestra **Modalità**.

2. Selezionare uno dei livelli di sicurezza suggeriti (vedere la figura sotto).

Figura 53. Selezione del livello di sicurezza di Firewall

3. Premere **Indietro** per salvare le modifiche.

NOTIFICA DEL TENTATIVO DI CONNESSIONE

La funzione Firewall blocca tutte le connessioni bloccate in base alla modalità di sicurezza selezionata (vedere la sezione "Selezione del livello di sicurezza di Firewall" a pagina 90). Per specificare a Firewall di informare l'utente delle connessioni bloccate sul dispositivo mobile, utilizzare la notifica Firewall.

➡ *Per ricevere informazioni sui tentativi di connessione bloccati al livello di sicurezza di Firewall selezionato, eseguire le seguenti operazioni:*

1. Nella scheda **Firewall**, selezionare l'opzione **Notifica**.

2. Selezionare il valore **Notifica** per l'impostazione **In caso di blocco** (vedere la figura sotto).

Figura 54. Configurazione delle notifiche di Firewall

3. Premere **OK** per salvare le modifiche.

CRIPTAGGIO DEI DATI PERSONALI

Questa sezione fornisce informazioni sul componente Criptaggio che protegge i dati riservati sul dispositivo. La sezione spiega inoltre come abilitare/disabilitare il funzionamento del componente e come criptare/decriptare le cartelle selezionate.

IN QUESTA SEZIONE

Informazioni sul componente Criptaggio 92

Criptaggio dei dati..... 93

Decriptaggio dei dati..... 94

Blocco dell'accesso ai dati criptati 95

INFORMAZIONI SUL COMPONENTE CRIPTAGGIO

Kaspersky Mobile Security 9.0 non supporta il criptaggio dei dati sui dispositivi mobili basati su Symbian Serie 60 5a Edizione.

Il componente Criptaggio protegge i dati sul dispositivo dalla visualizzazione da parte di altre persone che riescano ad avere accesso al dispositivo mobile. Il componente consente di criptare qualsiasi numero di cartelle non di sistema.

Per decriptare i dati, è necessario immettere la password segreta. Dopo il passaggio del dispositivo alla modalità di risparmio energia, alla scadenza dell'ora impostata (vedere la sezione "Protezione dell'accesso ai dati criptati " a pagina 95), l'accesso ai dati viene automaticamente bloccato.

I dati nella cartella verranno criptati i dopo l'esecuzione del comando **Cripta**. Successivamente, i dati verranno criptati e decriptati in tempo reale quando vengono spostati in una cartella, estratti da essa o al loro accesso.

Al termine dell'installazione, il componente Criptaggio di Kaspersky Mobile Security 9.0 è disabilitato.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

CRIPTAGGIO DEI DATI

Il componente Criptaggio consente di criptare qualsiasi numero di cartelle non di sistema presenti nella memoria del dispositivo o su una scheda di memoria.

L'elenco di tutti i file precedentemente criptati e decriptati è accessibile nella scheda **Criptaggio** da **Elenco cartelle**.

È possibile anche criptare immediatamente tutte le cartelle presenti nell'elenco delle cartelle.

Per criptare i dati:

1. Selezionare l'opzione **Elenco cartelle** nella scheda **Criptaggio**.

   Verrà aperta la finestra **Elenco cartelle**.

2. Selezionare **Opzioni → Aggiungi cartella** (vedere la figura sotto).

Figura 55. Criptaggio dei dati

   Verrà aperta una schermata contenente la struttura dei file del sistema del dispositivo.

3. Selezionare la cartella da criptare e avviare il processo di criptaggio della cartella selezionata. Per eseguire questa operazione, premere **Opzioni → Cripta**.

   Per spostarsi nel file system, utilizzare la penna a stilo o i pulsanti di spostamento del dispositivo come indicato di seguito: **Su** e **Giù** per spostarsi all'interno della cartella selezionata, **Sinistra** e **Destra** per spostarsi più in alto o più in basso di un livello rispetto alla cartella corrente.

4. Premere **OK**.

   La cartella criptata verrà aggiunta all'elenco delle cartelle.

Al termine del processo di criptaggio , il nome dell'opzione **Cripta** cambia in **Decripta** nel menu **Opzioni**.

Dopo il processo di criptaggio , i dati verranno decriptati e criptati automaticamente alla loro apertura o spostamento dalla cartella criptata , oppure se si collocano nuovi dati nella cartella criptata .

- *Per criptare in un solo passaggio tutte le cartelle presenti nell'elenco, eseguire le seguenti operazioni:*

1. Nella scheda **Criptaggio**, selezionare **Elenco cartelle**.

   Verrà aperta la finestra **Elenco cartelle**.

2. Selezionare **Opzioni** → **Aggiungi azioni** → **Cripta tutto**.

3. Premere **OK**.

DECRIPTAGGIO DEI DATI

È possibile decriptare completamente i dati criptati precedentemente (vedere la sezione "Criptaggio dei dati" a pagina 93). È possibile decriptare una o tutte le cartelle criptate presenti sul dispositivo.

- *Per decriptare una cartella precedentemente criptata:*

1. Selezionare l'opzione **Elenco cartelle** nella scheda **Criptaggio**.

   Verrà aperta la finestra **Elenco cartelle** contenente un elenco di tutte le cartelle precedentemente decriptate e criptate.

2. Selezionare dall'elenco la cartella che si desidera decriptare e selezionare **Opzioni** → Decripta (vedere la figura sotto).

Figura 56. Decriptaggio dei dati

3. Al completamento della decriptazione dei dati, premere **OK**.

Al termine del processo di criptaggio , il nome dell'opzione Decripta cambia in **Cripta** nel menu **Opzioni**. È possibile a questo punto criptare nuovamente i dati (vedere la sezione "Criptaggio dei dati" a pagina 93).

Per decriptare in un solo passaggio tutte le cartelle presenti nell'elenco, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Elenco cartelle** nella scheda **Criptaggio**.

   Verrà aperta la finestra **Elenco cartelle**.

2. Selezionare **Opzioni** → **Aggiungi azioni** →**Decripta tutto**.

3. Premere **OK**.

BLOCCO DELL'ACCESSO AI DATI CRIPTATI

Il componente Criptaggio consente di bloccare l'accesso ai dati criptati immediatamente o alla scadenza dell'ora impostata dopo aver posto il dispositivo in modalità di risparmio energia.

Per impostazione predefinita, l'accesso ai dati criptati viene bloccato immediatamente dopo aver disabilitato la retroilluminazione.

È possibile impostare un'ora durante la quale i dati criptati rimangono accessibili dopo che il dispositivo è passato in modalità di risparmio energia. Per continuare ad utilizzare i dati criptati , è necessario immettere la password segreta.

È possibile anche inibire momentaneamente l'accesso ai dati criptati e abilitare la richiesta della password segreta.

Per inibire l'accesso alla cartella con un ritardo temporale, eseguire le seguenti operazioni:

1. Nella scheda **Criptaggio**, selezionare l'opzione **Blocca accesso**.

   Verrà aperta la finestra **Blocca accesso**.

2. Immettere il tempo dopo il quale il dispositivo entra in standby e in cui i dati sono accessibili. Per eseguire questa operazione, selezionare uno dei valori suggeriti (vedere la figura sotto):

   - **Nessun ritardo**.
   - **Dopo 1 minuto**.
   - **Dopo 5 minuti**.
   - **Dopo 15 minuti**.

- **Dopo 1 ora**.

Figura 57. Blocco dell'accesso ai dati criptati

3. Premere **OK** per salvare le modifiche.

Per inibire l'accesso ai dati criptati e contemporaneamente abilitare la richiesta della password segreta,

premere contemporaneamente "0" e "1".

AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

Questa sezione fornisce informazioni sull'aggiornamento dei database dell'applicazione, che assicura la protezione aggiornata del dispositivo. La sezione specifica inoltre come visualizzare informazioni sui database dell'applicazione installati, come avviare manualmente il processo di aggiornamento e come configurare gli aggiornamenti automatici del database.

IN QUESTA SEZIONE

Informazioni sull'aggiornamento dei database dell'applicazione 97

Visualizzazione delle informazioni sul database 97

Avvio di aggiornamenti manuale 98

Avvio di aggiornamenti pianificati 99

Aggiornamento in roaming 100

Configurazione delle impostazioni di connessione a Internet 101

INFORMAZIONI SULL'AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

L'applicazione esegue la scansione del dispositivo per individuare eventuali programmi malware utilizzando il database dell'applicazione, che contiene le descrizioni di tutti i programmi malware e di altri programmi indesiderati noti attualmente e i metodi per neutralizzarli. È quindi estremamente importante tenere aggiornato il database.

Si consiglia di aggiornare regolarmente i database dell'applicazione. Trascorsi più di 15 giorni dall'ultimo aggiornamento, i database verranno considerati come molto vecchi. Sarà quindi impossibile garantire una protezione affidabile.

Kaspersky Mobile Security 9.0 esegue l'aggiornamento dai server di aggiornamento di Kaspersky Lab. Si tratta di siti Internet dedicati contenenti gli aggiornamenti per i database di tutti i prodotti Kaspersky Lab.

Per aggiornare i database dell'applicazione è necessario disporre di una connessione Internet configurata sul proprio dispositivo mobile.

I database dell'applicazione vengono aggiornati mediante il seguente algoritmo:

1. I database dell'applicazione installati sul dispositivo mobile vengono confrontati a quelli situati sul server di aggiornamento dedicato di Kaspersky Lab.

2. Kaspersky Mobile Security 9.0 esegue una delle seguenti operazioni:

   - Se sono installati i database dell'applicazione più recenti, sullo schermo viene visualizzato un messaggio informativo.

   - Se i database installati sono diversi, viene scaricato e installato un nuovo pacchetto di aggiornamento.

     Al termine del processo di aggiornamento, la connessione viene automaticamente chiusa. Se la connessione è stata stabilita prima dell'avvio dell'aggiornamento, rimarrà aperta per ulteriore utilizzo.

Le impostazioni di connessione a Internet vengono definite automaticamente per impostazione predefinita. Se le impostazioni di connessione a Internet non vengono definite automaticamente, configurarle (vedere la sezione "Configurazione delle impostazioni di connessione a Internet" a pagina 101).

È possibile avviare l'operazione di aggiornamento manualmente in qualsiasi momento mentre il dispositivo è occupato con altre operazioni oppure pianificare aggiornamenti automatici.

Quando il dispositivo è in roaming, è possibile disabilitare l'aggiornamento dei database di Kaspersky Mobile Security 9.0 per evitare costi indesiderati.

La data di rilascio del database è visibile nella finestra di stato della protezione (vedere la sezione "Finestra Stato di protezione" a pagina 34). Informazioni dettagliate sui database sono disponibili nella scheda **Avanzate** della voce del menu **Info database**.

Le informazioni sugli aggiornamenti dei database vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

VISUALIZZAZIONE DELLE INFORMAZIONI SUL DATABASE

È possibile visualizzare informazioni sui database dell'applicazione installati. Sono disponibili le seguenti informazioni: data dell'ultimo aggiornamento, data di rilascio dei database e numero di voci nei database.

- *Per visualizzare le informazioni sui database installati,*

  selezionare l'opzione **Info database** nella scheda **Avanzate** (vedere la figura sotto).

Figura 58. Informazioni sui database dell'applicazione installati

AVVIO DI AGGIORNAMENTI MANUALE

È possibile avviare manualmente l'aggiornamento dei database dell'applicazione.

- *Per avviare manualmente il processo di aggiornamento del database:*

  1. Selezionare l'opzione **Aggiornamento** nella scheda **Anti-Virus**.

     Verrà aperta la finestra **Aggiornamento**.

2. Selezionare l'opzione **Aggiornamento** (vedere la figura sotto).

Figura 59. Avvio manuale dell'aggiornamento

L'applicazione avvia il processo di aggiornamento dei database dal server Kaspersky Lab. Le informazioni sul processo di aggiornamento vengono visualizzate sullo schermo.

AVVIO DI AGGIORNAMENTI PIANIFICATI

L'esecuzione regolare degli aggiornamenti è il requisito di base per l'efficace protezione del dispositivo contro le infezioni di oggetti malware. Per maggiore comodità, è possibile configurare aggiornamenti automatici del database.

È possibile inoltre configurare impostazioni di aggiornamento automatico quando il dispositivo si trova in a zona roaming (vedere la sezione "Aggiornamento in roaming" a pagina 100).

Per configurare una pianificazione per gli aggiornamenti automatici del database:

1. Selezionare l'opzione **Aggiornamento** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Aggiornamento**.

2. Selezionare l'opzione **Pianifica**.

   Verrà aperta la finestra **Pianifica**.

3. Selezionare per l'impostazione **Aggiornamento autom.** uno dei valori suggeriti (vedere la figura sotto):

   - **Disabilitato**: non aggiorna il database dell'applicazione in base a una pianificazione.
   - **Settimanale**: esegue l'aggiornamento una volta alla settimana. Selezionare quindi un valore per le impostazioni **Giorno aggiornamento** e **Ora aggiornamento**.

- **Giornaliero**: aggiorna il database dell'applicazione ogni giorno. Immettere quindi un valore per l'impostazione **Ora aggiornamento**.

Figura 60. Impostazioni di aggiornamento automatico

4. Premere **Indietro** per salvare le modifiche.

AGGIORNAMENTO IN ROAMING

Quando il dispositivo si trova in una zona roaming, è possibile disabilitare gli aggiornamenti pianificati del database dell'applicazione. L'aggiornamento manuale sarà comunque disponibile in modalità normale.

Per disabilitare gli aggiornamenti pianificati quando il dispositivo si trova in una zona roaming, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Aggiornamento** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Aggiornamento**.

2. Selezionare l'opzione **Pianifica**.

   Verrà aperta la finestra **Pianifica**.

3. Selezionare per l'impostazione **Consenti in roaming** il valore **No** (vedere la figura sotto).

Figura 61. Configurazione degli aggiornamenti in roaming

4. Premere **Indietro** per salvare le modifiche.

CONFIGURAZIONE DELLE IMPOSTAZIONI DI CONNESSIONE A INTERNET

Per la connessione a Internet, Kaspersky Mobile Security 9.0 utilizza un punto di accesso predefinito.

Le impostazioni del punto di accesso vengono definite dal fornitore.

Se in Kaspersky Mobile Security 9.0 non sono specificate automaticamente le impostazioni di connessione, configurale.

➡ *Per configurare le impostazioni di connessione a Internet, eseguire le seguenti operazioni:*

1. Selezionare l'opzione **Aggiornamento** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Aggiornamento**.

2. Selezionare l'opzione **Connessione**.

3. Selezionare il punto di accesso che verrà utilizzato per la connessione al server di aggiornamento. Per eseguire questa operazione, selezionare un valore per l'impostazione **Punto di accesso** e premere **OK** (vedere la figura sotto).

   L'elenco mostra tutti i punti di accesso impostati sul dispositivo mobile.

Figura 62. Impostazioni di connessione a Internet

4. Premere **Indietro** per salvare le modifiche.

REPORT DELL'APPLICAZIONE

Questa sezione fornisce informazioni sui report in cui viene registrato il funzionamento di ogni componente e l'esecuzione di ogni attività (ad esempio, gli aggiornamenti del database dell'applicazione, le scansioni anti-virus, ecc.).

IN QUESTA SEZIONE

Informazioni sui report 102

Visualizzazione dei record del report 103

Eliminazione dei record del report 103

INFORMAZIONI SUI REPORT

Nei report dell'applicazione vengono memorizzati i record relativi agli eventi che si verificano durante il funzionamento di Kaspersky Mobile Security. Le voci vengono ordinate in base all'ora dell'evento e a partire dagli eventi più recenti.

Per ogni componente viene utilizzato un report eventi distinto.

VISUALIZZAZIONE DEI RECORD DEL REPORT

- *Per visualizzare le voci nel report del componente, eseguire le seguenti operazioni:*

1. Nella scheda del componente desiderato, selezionare l'opzione **Report**.

   Verrà aperto il report del componente selezionato (vedere la figura sotto).

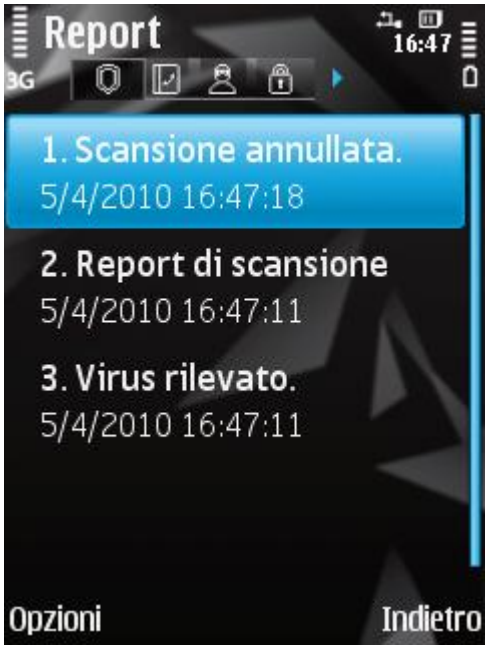


Figura 63. Report del componente selezionato

2. Utilizzare i pulsanti di spostamento per spostarsi nel report: **su** e **giù**: visualizzano gli eventi nel report corrente, **Sinistra** e **destra**: visualizzano gli eventi nei report degli altri componenti.

- *Per visualizzare informazioni dettagliate sui record del report,*

  selezionare la voce desiderata e selezionare **Opzioni** → **Mostra informazioni**.

ELIMINAZIONE DEI RECORD DEL REPORT

È possibile svuotare tutti i report. Le informazioni sul funzionamento di tutti i componenti di Kaspersky Mobile Security 9.0 verranno eliminate.

- *Per eliminare tutte le voci dal report, eseguire le seguenti operazioni:*

1. Nella scheda di un componente, selezionare l'opzione **Report**.

   Verrà aperta la finestra **Report**.

2. Selezionare **Opzioni** → **Svuota report**.

Verranno eliminati tutti i record in tutti i report dei componenti.

CONFIGURAZIONE DI IMPOSTAZIONI AGGIUNTIVE

Questa sezione fornisce informazioni sulle opzioni aggiuntive di Kaspersky Mobile Security 9.0: come gestire le notifiche acustiche dell'applicazione e la retroilluminazione dello schermo, e come abilitare/disabilitare la visualizzazione dei suggerimenti, dell'icona Protezione e la finestra Stato di protezione.

IN QUESTA SEZIONE

Modifica della password segreta 104

Visualizzazione dei suggerimenti 104

Configurazione delle notifiche acustiche 105

Gestione della retroilluminazione 106

Visualizzazione della finestra di stato 106

Visualizzazione dell'icona Protezione 107

MODIFICA DELLA PASSWORD SEGRETA

È possibile modificare la password segreta impostata dopo l'attivazione dell'applicazione.

Per modificare la password segreta:

1. Selezionare l'opzione **Impostazioni** nella scheda **Avanzate**.

   Verrà aperta la finestra **Impostazioni**.

2. Selezionare l'impostazione **Cambia password**.

3. Immettere il codice corrente nel campo **Immetti password** e premere **OK**.

4. Immettere la nuova password nel campo **Immettere nuova password** e premere **OK** per salvare le modifiche.

VISUALIZZAZIONE DEI SUGGERIMENTI

Quando si configurano le impostazioni dei componenti, Kaspersky Mobile Security 9.0 visualizza un messaggio predefinito con una descrizione sintetica della funzione selezionata. È possibile configurare la visualizzazione dei suggerimenti di Kaspersky Mobile Security 9.0.

Per configurare la visualizzazione dei suggerimenti, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Impostazioni** nella scheda **Avanzate**.

   Verrà aperta la finestra **Impostazioni**.

2. Selezionare uno dei valori suggeriti per l'impostazione **Suggerimenti**:

   - **Mostra**: visualizza i suggerimenti prima di configurare le impostazioni della funzione selezionata.
   - **Nascondi**: non visualizza i suggerimenti.

3. Premere **Indietro** per salvare le modifiche.

CONFIGURAZIONE DELLE NOTIFICHE ACUSTICHE

In seguito al funzionamento dell'applicazione, si verificano eventi specifici: ad esempio, è stato rilevato un oggetto infetto o un virus, il periodo di validità della licenza sta per scadere, ecc. Per specificare all'applicazione di informare l'utente di ogni evento del genere, è possibile abilitare l'emissione di notifiche acustiche al verificarsi degli eventi.

Per impostazione predefinita, Kaspersky Mobile Security 9.0 emette le notifiche acustiche solo in base alla modalità impostata sul dispositivo.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per gestire l'emissione di notifiche acustiche dell'applicazione, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Impostazioni** nella scheda **Avanzate**.

   Verrà aperta la finestra **Impostazioni**.

2. Selezionare uno dei valori suggeriti per l'impostazione **Notifiche acustiche** (vedere la figura sotto):

   - **Sempre**: emette notifiche acustiche indipendentemente dal profilo del dispositivo selezionato.
   - **In base al profilo**: emette notifiche acustiche in base alla modalità del dispositivo selezionata.
   - **Disabilita**: non emette notifiche acustiche.

Figura 64. Gestione delle notifiche acustiche

3. Premere **Indietro** per salvare le modifiche.

GESTIONE DELLA RETROILLUMINAZIONE

Quando l'applicazione esegue le attività di protezione, viene consumata una quantità elevata di energia. Per risparmiare energia durante l'esecuzione di queste attività, l'applicazione consente di disabilitare automaticamente la retroilluminazione dello schermo.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per configurare la retroilluminazione dello schermo durante l'esecuzione della attività, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Impostazioni** nella scheda **Avanzate**.

   Verrà aperta la finestra **Impostazioni**.

2. Selezionare uno dei valori suggeriti per l'impostazione **Retroilluminazione** (vedere la figura sotto):

   - **In base al profilo**: utilizza la retroilluminazione dello schermo in base alla modalità del dispositivo selezionata.
   - **Abilita**: utilizza sempre la retroilluminazione dello schermo.

Figura 65. Gestione della retroilluminazione

3. Premere **Indietro** per salvare le modifiche.

VISUALIZZAZIONE DELLA FINESTRA DI STATO

È possibile scegliere se visualizzare o meno la finestra di stato dell'applicazione all'avvio.

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per configurare la finestra di stato all'avvio dell'applicazione, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Impostazioni** nella scheda **Avanzate**.

   Verrà aperta la finestra **Impostazioni**.

2. Selezionare uno dei valori suggeriti per l'impostazione **Schermata di stato** (vedere la figura sotto):

   - **Mostra**: mostra la finestra di stato.
   - **Nascondi**: non mostra la finestra di stato.

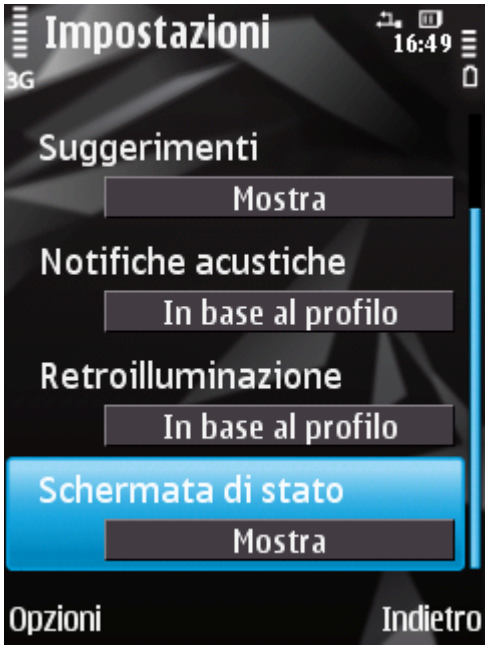


Figura 66. Configurazione della visualizzazione della finestra di stato

3. Premere **Indietro** per salvare le modifiche.

VISUALIZZAZIONE DELL'ICONA PROTEZIONE

Per visualizzare lo stato della protezione, è possibile configurare la visualizzazione dell'icona Protezione sullo schermo del dispositivo mobile (vedere la sezione "Icona Protezione" a pagina 33).

Per modificare le impostazioni, è possibile utilizzare i pulsanti di spostamento del dispositivo o selezionare **Opzioni** → **Cambia**.

Per modificare le impostazioni di visualizzazione dell'icona Protezione, eseguire le seguenti operazioni:

1. Selezionare l'opzione **Protezione** nella scheda **Anti-Virus**.

   Verrà aperta la finestra **Protezione**.

2. Selezionare uno dei valori suggeriti per l'impostazione **Icona Protezione** (vedere la figura sotto):

   - **Mostra sempre**: mostra l'icona Protezione sullo schermo del dispositivo.
   - **Solo nel menu**: mostra l'icona Protezione solo quando è aperto il menu del dispositivo o il menu di Kaspersky Mobile Security 9.0.

- **Non mostrare**: non mostra l'icona Protezione.

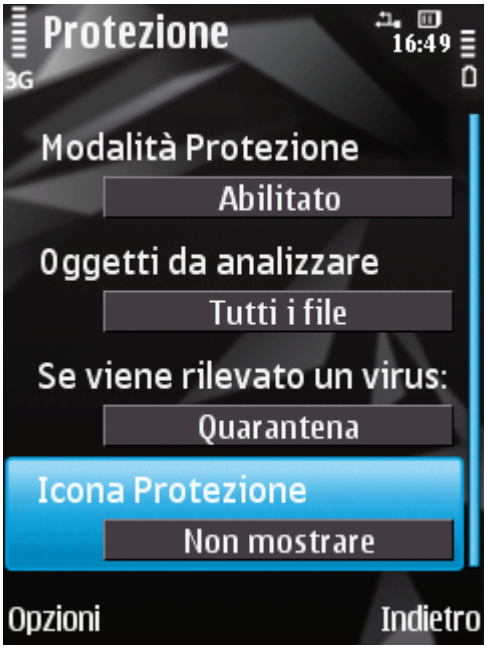


Figura 67. Impostazioni di visualizzazione dell'icona Protezione

3. Premere **OK** per salvare le modifiche.

KASPERSKY MOBILE SECURITY 9.0 PER MICROSOFT WINDOWS MOBILE

Questa sezione descrive il funzionamento di Kaspersky Mobile Security per dispositivi mobili basati su uno dei seguenti sistemi operativi:

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0, 6.1, 6.5.

IN QUESTA SEZIONE

Installazione di Kaspersky Mobile Security 9.0 109

Disinstallazione dell'applicazione 110

Aggiornamento dalla versione 8.0 alla versione 9.0 112

Operazioni preliminari 113

Interfaccia dell'applicazione 123

Protezione del file system 126

Scansione del dispositivo 129

Quarantena degli oggetti malware 136

Filtro delle chiamate e dei messaggi SMS in entrata 138

Limitazione delle chiamate e dei messaggi SMS in uscita. Parental Control 151

Protezione dei dati in caso di smarrimento o furto del dispositivo 159

Mascheramento dei dati personali 170

Filtro dell'attività di rete. Firewall 179

Criptaggio dei dati personali 181

Aggiornamento dei database dell'applicazione 186

Report dell'applicazione 191

Configurazione di impostazioni aggiuntive 193

INSTALLAZIONE DI KASPERSKY MOBILE SECURITY 9.0

L'installazione dell'applicazione su un dispositivo mobile viene eseguita mediante alcuni passaggi.

Prima di avviare l'installazione, si consiglia di chiudere tutte le altre applicazioni in esecuzione.

Per installare Kaspersky Mobile Security 9.0:

1. Collegare il dispositivo mobile al computer utilizzando l'applicazione Microsoft ActiveSync.

2. Eseguire una delle seguenti operazioni:

   - Se si è acquistato il programma su CD, eseguire l'installazione automatica di Kaspersky Mobile Security 9.0 dal CD acquistato.

   - Se si è acquistato il pacchetto di distribuzione su Internet, copiarlo sul dispositivo mobile utilizzando uno dei seguenti metodi:

     - dal sito Web di Kaspersky Lab;

     - utilizzando l'applicazione Microsoft ActiveSync;

     - utilizzando una scheda di espansione di memoria.

     Eseguire l'installazione aprendo l'archivio cab contenente il pacchetto di distribuzione sul dispositivo mobile.

3. Leggere il testo del Contratto di licenza che intercorre tra l'utente e Kaspersky Lab. Per accettare tutti i termini del contratto, premere **OK**. Kaspersky Mobile Security 9.0 verrà installato sul dispositivo. Se non si accettano i termini del Contratto di licenza, premere **Annulla**.

4. Selezionare la lingua dell'interfaccia di Kaspersky Mobile Security 9.0 e premere **OK**.

5. Riavviare il dispositivo per completare l'installazione. premendo **Riavvia**.

   L'applicazione viene installata con i parametri consigliati dagli esperti di Kaspersky Lab.

DISINSTALLAZIONE DELL'APPLICAZIONE

Per disinstallare Kaspersky Mobile Security 9.0:

1. Decriptare i dati sul dispositivo se questi sono stati criptati con Kaspersky Mobile Security 9.0 (vedere la sezione "Decriptaggio dei dati" a pagina 183).

2. Disabilitare il componente Protezione privacy (vedere la sezione "Abilitazione/disabilitazione del componente Protezione privacy" a pagina 172).

3. Chiudere Kaspersky Mobile Security 9.0 premendo **Menu** → **Esci**.

4. Disinstallare di Kaspersky Mobile Security 9.0 eseguendo le seguenti operazioni:

   a. Premere **Start** → **Impostazioni**.

b. Selezionare **Disinstallaz. applicazioni** nella scheda **Sistema** (vedere la figura sotto).

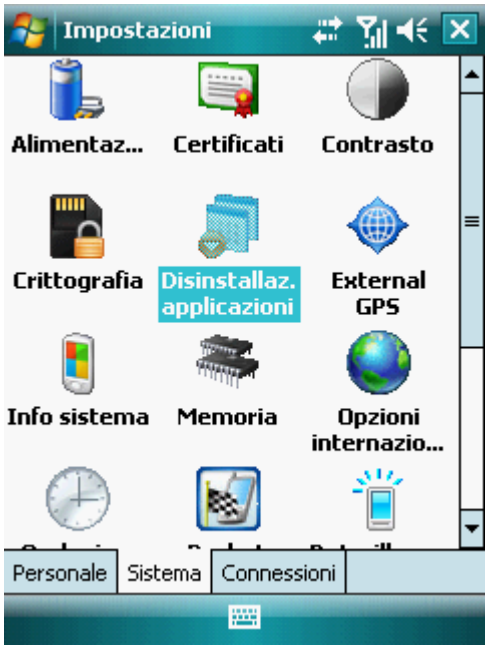


*Figura 68. Scheda **Sistema***

c. Selezionare **Kaspersky Mobile Security** dall'elenco dei programmi installati e premere il pulsante **Rimuovi** (vedere la figura sotto).

Figura 69. Selezione dell'applicazione da disinstallare

d. Nella finestra visualizzata, confermare la disinstallazione dell'applicazione premendo il pulsante **Sì**.

e. Immettere la password segreta e premere **OK**.

f. Specificare se conservare o meno le impostazioni del programma e gli oggetti in quarantena (vedere la figura sotto):

- Per conservare le impostazioni dell'applicazione e gli oggetti in quarantena, premere **Conserva** (vedere la figura sotto).
- Per disinstallare completamente l'applicazione, premere **Elimina**.

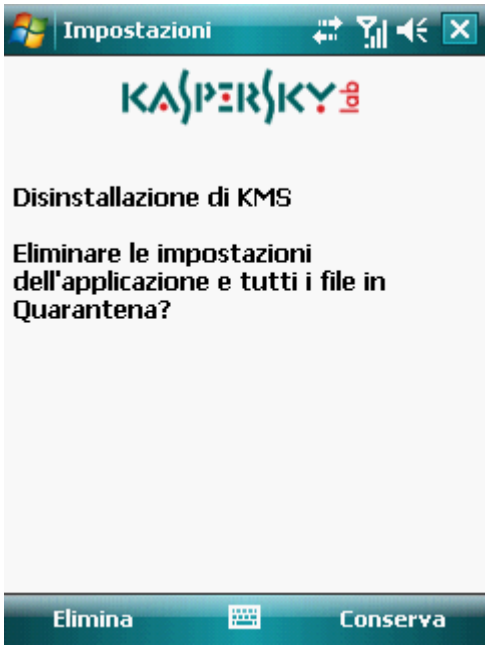


Figura 70. Rimozione delle impostazioni dell'applicazione

5. Riavviare il dispositivo per completare la disinstallazione dell'applicazione.

AGGIORNAMENTO DALLA VERSIONE 8.0 ALLA VERSIONE 9.0

Se sul dispositivo mobile è già installato Kaspersky Mobile Security 8.0, è possibile aggiornarlo alla versione 9.0.

Prima di aggiornare la versione dell'applicazione, disabilitare Criptaggio – decripta tutti i dati (vedere la sezione "Decriptaggio dei dati" a pagina 183).

Per aggiornare la versione del programma:

1. Chiudere la versione corrente di Kaspersky Mobile Security premendo **Menu** → **Esci**.
2. Copiare il pacchetto di distribuzione dell'applicazione sul dispositivo utilizzando uno dei seguenti metodi:
   - dal sito Web di Kaspersky Lab;
   - utilizzando l'applicazione Microsoft ActiveSync;
   - utilizzando una scheda di espansione di memoria.
3. Avviare il pacchetto di distribuzione di Kaspersky Mobile Security 9.0 sul dispositivo.
4. Leggere attentamente il contratto di licenza. Per accettare i termini del contratto, premere **OK**. Verrà chiesto di disinstallare prima la versione 8.0.
5. Confermare la disinstallazione della versione 8.0 dell'applicazione premendo il pulsante **OK**.

6. Immettere la password segreta impostata nella versione precedente dell'applicazione.

7. Eliminare le impostazioni configurate della versione precedente dell'applicazione premendo **Elimina**.

Le impostazioni possono essere salvate durante il passaggio da una versione all'altra nell'ambito della stessa generazione di prodotti. I parametri della versione 8.0 dell'applicazione non sono compatibili con la versione 9.0.

8. Riavviare il dispositivo per completare il processo di rimozione premendo **Riavvia**.

9. Dopo aver riavviato il dispositivo, eseguire l'installazione di Kaspersky Mobile Security 9.0 (vedere la sezione "Installazione di Kaspersky Mobile Security 9.0" a pagina 109).

   Se il periodo di validità della licenza di Kaspersky Mobile Security 8.0 non è scaduto, abilitare la versione 9.0 del programma utilizzando il codice di attivazione della versione 8.0 (vedere la sezione "Attivazione dell'applicazione" a pagina 113).

OPERAZIONI PRELIMINARI

Questa sezione contiene informazioni su come preparare Kaspersky Mobile Security 9.0 per il funzionamento (attivazione e creazione di una password segreta), eseguire l'applicazione, aggiornare i suoi database ed eseguire la scansione anti-virus del dispositivo.

IN QUESTA SEZIONE

Attivazione dell'applicazione....113

Immissione della password segreta....116

Avvio dell'applicazione....117

Aggiornamento dei database dell'applicazione....117

Scansione anti-virus del dispositivo....118

Visualizzazione di informazioni sull'applicazione....118

Gestione della licenza....119

ATTIVAZIONE DELL'APPLICAZIONE

Per poter utilizzare Kaspersky Mobile Security 9.0, è necessario prima attivarlo. Durante il processo di attivazione, è necessario immettere un codice di attivazione che viene verificato e registrato sui server Kaspersky Lab. Successivamente, l'applicazione riceverà e installerà un file chiave.

È possibile ottenere un codice di attivazione nei seguenti modi:

- (vedere la sezione "Acquisto di un codice di attivazione online" a pagina 116), uscendo dall'applicazione Kaspersky Mobile Security 9.0 e accedendo al sito Web http://www.kasperskystore.it;
- sul sito Web all'indirizzo http://www.kasperskystore.it;
- dai distributori Kaspersky Lab.

Per attivare Kaspersky Mobile Security 9.0 sul proprio dispositivo è necessario disporre di una connessione Internet configurata.

Prima di attivare l'applicazione, assicurarsi che le impostazioni della data di sistema del dispositivo siano corrette.

È possibile attivare l'applicazione nei seguenti modi:

- **Attivare la licenza trial**. Selezionare questo metodo di attivazione se si desidera acquisire dimestichezza con le funzioni dell'applicazione e acquistare la versione commerciale in un secondo momento. Durante l'attivazione verrà installato un file chiave gratuito. Al completamento dell'attivazione, sullo schermo verrà visualizzato il periodo di validità della licenza trial. Alla scadenza del periodo di validità della licenza trial, le funzioni dell'applicazione saranno limitate. Saranno disponibili solo le seguenti funzioni:

  - attivazione dell'applicazione;
  - gestione della licenza dell'applicazione;
  - guida in linea di Kaspersky Mobile Security 9.0;
  - disabilitazione del componente Criptaggio;
  - disabilitazione del componente Protezione privacy.

  Non è possibile riattivare una licenza trial.

- **Attivare la licenza commerciale**. Selezionare questo metodo se si è acquistata la versione commerciale dell'applicazione e si è ottenuto un codice di attivazione. Dopo aver immesso il codice di attivazione, verrà ricevuto e installato un file chiave che fornisce l'accesso alla gamma completa delle funzioni dell'applicazione. Sullo schermo del dispositivo verrà visualizzato il periodo di validità. Alla scadenza del periodo di validità, le funzioni dell'applicazione saranno limitate; l'applicazione non verrà più aggiornata.

IN QUESTA SEZIONE

Attivazione della versione commerciale 114

Attivazione della versione trial 115

Acquisto online di un codice di attivazione 116

ATTIVAZIONE DELLA VERSIONE COMMERCIALE

Per attivare la versione commerciale dell'applicazione con il codice di attivazione:

1. Selezionare **Start** → **Programmi**.
2. Selezionare **KMS 9.0** ed eseguire l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.

   Verrà aperta la finestra **Attivazione**.
3. Selezionare **Immetti codice**.

   Verrà aperta la finestra di attivazione di Kaspersky Mobile Security 9.0 (vedere la figura sotto).

4. Successivamente, immettere il codice di attivazione ricevuto nei quattro campi, quindi selezionare **Avanti**.

Figura 71. Attivazione di una versione commerciale dell'applicazione

5. Confermare la connessione a Internet premendo **Sì**.

   L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e scaricherà e installerà il file chiave.

   Se per qualche motivo il codice di attivazione immesso non risulta valido, sullo schermo verrà visualizzato un messaggio informativo. In questo caso, si consiglia di verificare che il codice di attivazione immesso sia corretto e di contattare il rivenditore del software presso cui è stato acquistato Kaspersky Mobile Security 9.0.

   Se si sono verificati errori durante la connessione al server e non è stato possibile ottenere una chiave di licenza, l'attivazione verrà annullata. In questo caso, si consiglia di verificare i parametri di connessione a Internet. Se non è stato possibile correggere gli errori, contattare l'Assistenza tecnica.

6. Passare all'immissione della password segreta (vedere la sezione "Immissione della password segreta" a pagina 116).

ATTIVAZIONE DELLA VERSIONE TRIAL

➧ *Per attivare la licenza trial di Kaspersky Mobile Security 9.0:*

1. Selezionare **Start→ Programmi**.

2. Selezionare **KMS 9.0** ed eseguire l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.

   Verrà aperta la finestra **Attivazione**.

3. Selezionare **Versione trial**.

4. Confermare la connessione a Internet premendo **Sì**.

   L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e scaricherà e installerà il file chiave.

   Se si sono verificati errori durante la connessione al server e non è stato possibile ottenere una chiave di licenza, contattare l'Assistenza tecnica.

5. Passare all'immissione della password segreta (vedere la sezione "Immissione della password segreta" a pagina 116).

ACQUISTO ONLINE DI UN CODICE DI ATTIVAZIONE

Per acquistare online un codice di attivazione per l'applicazione, eseguire le seguenti operazioni:

1. Selezionare **Avvio→ Programmi**.
2. Selezionare **KMS 9.0** ed eseguire l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.

   Verrà aperta la finestra **Attivazione**.
3. Selezionare **Acquista online**.

   Verrà aperta la finestra **Acquista online**.
4. Premere **Apri**.

   Verrà aperto il sito Web http://www.kasperskystore.it in cui verrà chiesto di effettuare un ordine per il rinnovo della licenza.
5. Seguire le istruzioni dettagliate.
6. Al termine dell'acquisto del codice di attivazione, passare all'attivazione della versione commerciale dell'applicazione (vedere la sezione "Attivazione della versione commerciale" a pagina 114).

IMMISSIONE DELLA PASSWORD SEGRETA

Al termine dell'attivazione del programma, verrà chiesto di immettere la password segreta. La *password segreta* impedisce l'accesso non autorizzato alle impostazioni dell'applicazione. È possibile cambiare in un secondo momento la password segreta installata.

La password segreta viene richiesta nei seguenti casi:

- per l'accesso all'applicazione;
- per l'accesso ai dati criptati ;
- per abilitare/disabilitare il componente Protezione privacy;
- quando si invia un comando con uno speciale messaggio SMS per avviare le seguenti funzioni in remoto: SMS-Block, SMS-Clean, SIM Watch, SMS-Find, Protezione privacy;
- in caso di disinstallazione dell'applicazione.

Si raccomanda di non dimenticare la password segreta. Se si dimentica la password segreta, sarà impossibile utilizzare le funzioni di Kaspersky Mobile Security 9.0 oppure ottenere l'accesso ai dati criptati e disinstallare l'applicazione.

Si consiglia di scegliere una password segreta composta da almeno 7 cifre.

Per immettere la password segreta:

1. Al termine dell'attivazione dell'applicazione, immettere nel campo **Immettere nuova password** le cifre che comporranno la password.
2. Ripetere l'immissione dello stesso codice nel campo **Conferma**.

   Il codice immesso viene verificato automaticamente.
3. Se il codice viene considerato non valido in base ai risultati della verifica, verrà visualizzato un messaggio di avviso e l'applicazione richiederà una conferma. Per utilizzare il codice, premere **OK**. Per creare una nuova password, premere **No**.
4. Al completamento dell'operazione, premere **OK**.

AVVIO DELL'APPLICAZIONE

Per avviare Kaspersky Mobile Security 9.0:

1. Selezionare **Avvio** → **Programmi**.
2. Selezionare **KMS 9.0** ed eseguire l'applicazione utilizzando la penna a stilo o il pulsante centrale di spostamento.
3. Immettere la password segreta e premere **OK**.

L'applicazione visualizza una finestra che mostra lo stato corrente di Kaspersky Mobile Security 9.0 (vedere la sezione "Finestra Stato di protezione" a pagina 123). Per passare alle funzioni dell'applicazione, premere **Menu**.

AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

Kaspersky Mobile Security 9.0 esegue la scansione delle minacce in base ai database dell'applicazione, che contengono le descrizioni di tutti i programmi dannosi noti attualmente e i metodi per neutralizzarli, nonché le descrizioni di altri oggetti indesiderati. Al momento dell'installazione dell'applicazione, i database inclusi nel pacchetto di installazione di Kaspersky Mobile Security 9.0 possono risultare obsoleti.

Si consiglia di aggiornare i database dell'applicazione immediatamente dopo l'installazione dell'applicazione.

Per aggiornare i database dell'applicazione è necessario disporre di una connessione Internet configurata sul proprio dispositivo mobile.

Per avviare il processo di aggiornamento del database:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.
2. Selezionare l'opzione **Aggiornamento**.

   Verrà aperta la finestra **Aggiornamento**.
3. Selezionare l'opzione **Aggiornamento**.

L'applicazione avvia il processo di aggiornamento dei database dal server Kaspersky Lab. Le informazioni sul processo di aggiornamento vengono visualizzate sullo schermo.

SCANSIONE ANTI-VIRUS DEL DISPOSITIVO

Al termine dell'installazione dell'applicazione, si consiglia di eseguire immediatamente una scansione del dispositivo mobile per individuare eventuali oggetti malware.

La prima scansione viene eseguita con le impostazioni predefinite dagli esperti Kaspersky Lab.

Per eseguire una scansione completa del dispositivo:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

   Verrà aperta la finestra **Scansione**.

3. Selezionare **Scansione completa**.

VISUALIZZAZIONE DI INFORMAZIONI SULL'APPLICAZIONE

È possibile visualizzare informazioni di carattere generale sull'applicazione, comprendenti il numero di versione e dettagli sul copyright.

Per visualizzare le informazioni sulla licenza:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare la scheda **Info** (vedere la figura sotto).

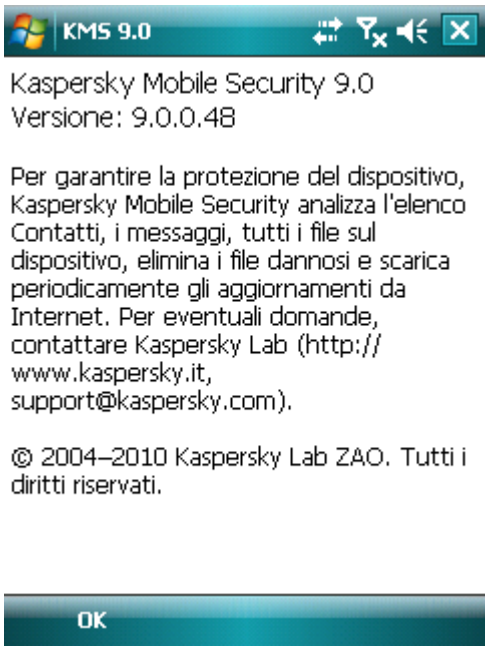


Figura 72. Informazioni sull'applicazione

GESTIONE DELLA LICENZA

Nell'ambito della gestione delle licenze delle applicazioni Kaspersky Lab, è importante conoscere i seguenti tre termini:

- Contratto di licenza;
- licenza;
- file chiave.

Tali termini sono inseparabilmente interconnessi e costituiscono un unico modello di gestione della licenza.

La seguente sezione descrive con maggiore dettaglio ognuno di questi termini.

La sezione spiega inoltre come reperire informazioni sulla licenza di Kaspersky Mobile Security 9.0 e su come estendere il suo periodo di validità.

IN QUESTA SEZIONE

Informazioni sul Contratto di licenza....119

Informazioni sulle licenze di Kaspersky Mobile Security....119

Informazioni sui file chiave di Kaspersky Mobile Security....120

Visualizzazione delle informazioni sulla licenza 121

Rinnovo della licenza....121

INFORMAZIONI SUL CONTRATTO DI LICENZA

Il *Contratto di licenza* è un accordo che intercorre tra Kaspersky Lab e la persona fisica o il soggetto giuridico che detiene legalmente una copia di Kaspersky Mobile Security. Tale contratto è incluso in ogni applicazione Kaspersky Lab e contiene informazioni dettagliate sui diritti e sulle limitazioni di utilizzo di Kaspersky Mobile Security.

Secondo quanto previsto dal Contratto di licenza, al momento dell'acquisto e dell'installazione di un'applicazione Kaspersky Lab, si ottiene il diritto illimitato di possederne la copia.

Kaspersky Lab offre inoltre i seguenti servizi aggiuntivi:

- assistenza tecnica;
- aggiornamento dei database di Kaspersky Mobile Security;
- moduli di programma dell'aggiornamento di Kaspersky Mobile Security.

Per poter usufruire di questi servizi, è necessario acquistare e attivare una licenza (vedere la sezione "Informazioni sulle licenze di Kaspersky Mobile Security" a pagina 119).

INFORMAZIONI SULLE LICENZE DI KASPERSKY MOBILE SECURITY

Una *licenza* consiste nel diritto di utilizzo di Kaspersky Mobile Security e di usufruire dei servizi aggiuntivi (vedere la sezione "Informazioni sul Contratto di licenza" a pagina 119) ad esso associati così come forniti da Kaspersky Lab o dai suoi partner.

Ogni licenza ha un periodo di validità distinto.

Il *periodo di validità della licenza* consiste nel periodo durante il quale vengono forniti all'utente servizi aggiuntivi. L'ambito dei servizi forniti dipende dal tipo di licenza.

Sono disponibili i seguenti tipi di licenza:

Trial, una licenza gratuita avente un periodo di validità limitato. Tale licenza viene offerta per consentire all'utente di conoscere e valutare Kaspersky Mobile Security. Viene fornita con una versione di prova dell'applicazione e ha un periodo di validità breve durante il quale l'utente può accedere alla Knowledge Base (http://www.kaspersky.com/it/service) e al forum (http://forum.kaspersky.com/index.php?showforum=62). Durante l'utilizzo dell'applicazione con licenza trial non è possibile contattare l'assistenza tecnica e al termine del suo periodo di validità non saranno più disponibili tutte le funzioni di Kaspersky Mobile Security.

Commerciale, una licenza a pagamento avente un periodo di validità normalmente non inferiore a un anno. Tale licenza viene concessa all'utente al momento dell'acquisto dell'applicazione. Al termine del periodo di validità della licenza commerciale di Kaspersky Mobile Security, alcune funzioni dell'applicazione diventeranno inaccessibili e i database dell'applicazione non verranno più aggiornati. In questo caso, la protezione completa del dispositivo non può essere garantita.

Per poter utilizzare l'applicazione e usufruire dei servizi aggiuntivi è necessario acquistare e attivare una licenza commerciale.

La licenza viene attivata installando il file chiave (vedere la sezione "Informazioni sui file chiave di Kaspersky Mobile Security" a pagina 120) collegato alla licenza.

INFORMAZIONI SUI FILE CHIAVE DI KASPERSKY MOBILE SECURITY

Il *file chiave* è un file che funge da chiave personale necessaria per l'utilizzo dell'applicazione. Il file chiave è un componente tecnologico che consente di attivare una licenza collegata ad esso e costituisce inoltre il diritto dell'utente di utilizzo dell'applicazione e dei servizi aggiuntivi.

Il file chiave è incluso nel kit di distribuzione dell'applicazione, se questa viene acquistata presso un rivenditore Kaspersky Lab, oppure viene inviato all'utente via e-mail, se l'applicazione viene acquistata sul negozio su Internet.

Il file chiave comprende le seguenti informazioni:

- Periodo di validità della licenza.
- Tipo di licenza (trial, commerciale).
- Limitazioni della licenza (ad esempio, numero di computer su cui la licenza è valida o volume del traffico e-mail protetto).
- Contatti di assistenza tecnica.
- Periodo di validità del file chiave.

Il *periodo di validità del file chiave*, ossia la data di scadenza associata al file chiave al momento della sottoscrizione, consiste nel periodo alla scadenza del quale il file chiave perde di validità con conseguente disabilitazione dell'opzione di attivazione della licenza ad esso associata.

Di seguito è fornito un esempio di come il periodo di validità del file chiave è collegato al periodo di validità della licenza.

Esempio:

Periodo di validità della licenza: 300 giorni

Data di sottoscrizione del file chiave: 01.09.2009

Periodo di validità del file chiave: 300 giorni

Data di installazione del file chiave (attivazione della licenza): 10.09.2009, ossia 9 giorni dopo la data di sottoscrizione.

Risultato:

Periodo di validità della licenza calcolato: 300 giorni – 9 giorni = 291 giorni.

VISUALIZZAZIONE DELLE INFORMAZIONI SULLA LICENZA

È possibile visualizzare le seguenti informazioni sulla licenza: file chiave, tipo, numero di giorni mancanti alla scadenza e numero del dispositivo.

Per visualizzare le informazioni sulla licenza:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Licenza**.

   Verrà aperta la finestra **Licenza**.

3. Selezionare **Info licenza**.

RINNOVO DELLA LICENZA

Kaspersky Mobile Security 9.0 consente di estendere la licenza dell'applicazione.

La licenza può essere estesa in uno dei seguenti modi:

- **Online**: attivando la licenza con una durata di un anno tramite il sito Web dedicato.
- **Tramite il codice di attivazione**, attivando l'applicazione con il codice di attivazione. È possibile acquistare il codice di attivazione su http://www.kasperskystore.it/cata_home.html oppure presso il proprio rivenditore Kaspersky Lab locale.

Per attivare l'applicazione sul proprio dispositivo mobile è necessario disporre di una connessione Internet configurata.

IN QUESTA SEZIONE

Rinnovo della licenza tramite il codice di attivazione 121

Rinnovo della licenza online 122

RINNOVO DELLA LICENZA TRAMITE IL CODICE DI ATTIVAZIONE

Per rinnovare la licenza tramite il codice di attivazione:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Licenza**.

   Verrà aperta la finestra **Licenza**.

3. Selezionare l'opzione **Rinnovo**.

   Verrà aperta la finestra **Rinnovo**.

4. Successivamente, immettere il codice di attivazione ricevuto nei quattro campi, quindi selezionare **Avanti**(vedere la figura sotto).

Figura 73. Rinnovo della licenza tramite il codice di attivazione

5. Confermare la connessione a Internet premendo **Sì**.

   L'applicazione invierà una richiesta al server di attivazione di Kaspersky Lab e scaricherà e installerà il file chiave. Se il file chiave viene installato correttamente, sullo schermo verranno visualizzate informazioni sulla licenza.

   Se per qualche motivo il codice di attivazione immesso non risulta valido, sullo schermo verrà visualizzato un messaggio corrispondente.

6. Al completamento dell'operazione, premere **OK**.

RINNOVO DELLA LICENZA ONLINE

Per rinnovare la licenza online:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Licenza**.

   Verrà aperta la finestra **Licenza**.

3. Selezionare l'opzione **Rinnova online**. Se il periodo di validità è scaduto, la voce del menu cambia in **Acquista online**.

   Verrà aperta la finestra **Rinnova online**.

4. Premere **Apri** (vedere la figura sotto).

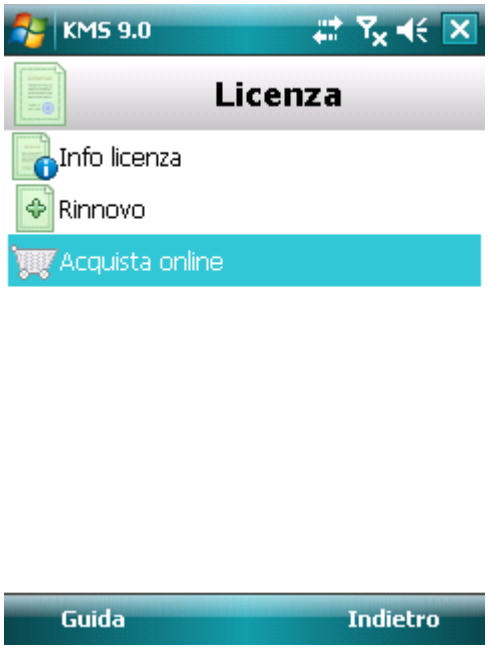


Figura 74. Rinnovo della licenza online

Verrà aperto il sito Web in cui verrà chiesto di effettuare un ordine per il rinnovo della licenza.

Se il periodo di validità è scaduto, verrà aperto il sito Web http://www.kasperskystore.it in cui è possibile acquistare il codice di attivazione online.

5. Seguire le istruzioni dettagliate.

6. Una volta elaborato l'ordine di rinnovo della licenza, immettere il codice di attivazione ricevuto (vedere la sezione "Rinnovo della licenza tramite il codice di attivazione" a pagina 121).

INTERFACCIA DELL'APPLICAZIONE

L'interfaccia di Kaspersky Mobile Security 9.0 è semplice e di facile utilizzo. Questa sezione fornisce informazioni sui suoi elementi principali.

IN QUESTA SEZIONE

Finestra Stato di protezione.....123

Menu dell'applicazione 125

FINESTRA STATO DI PROTEZIONE

Lo stato dei componenti principali dell'applicazione viene visualizzato nella finestra di stato corrente.

Per ciascun componente vi sono tre stati possibili, ognuno dei quali viene visualizzato con un colore specifico simile a quello dei semafori stradali. Il colore verde indica che la protezione del dispositivo è al livello necessario. I colori giallo e rosso indicano che vi sono vari livelli di minaccia della sicurezza. Le minacce non sono causate solo da programmi malware, ma derivano anche da database dell'applicazione obsoleti, dalla disabilitazione di alcuni componenti di protezione, da impostazioni di funzionamento dell'applicazione minime, ecc.

La finestra di stato è accessibile immediatamente dopo aver avviato l'applicazione e contiene le seguenti informazioni:

- **Protezione** è lo stato della protezione in tempo reale (vedere la sezione "Protezione del file system" a pagina 126).

  L'icona di stato verde indica che la protezione è attiva e garantita al livello richiesto, e che i database dell'applicazione sono aggiornati.

  L'icona di colore giallo indica che i database non sono stati aggiornati da vari giorni.

  L'icona di colore rosso indica problemi che possono causare perdita di informazioni o infezione del dispositivo. Ad esempio, la protezione è disattivata. L'applicazione potrebbe non essere stata aggiornata da molto tempo.

- **Firewall** è il livello di protezione del dispositivo da attività di rete indesiderate (vedere la sezione "Filtro dell'attività di rete. Firewall" a pagina 179).

  L'icona di stato verde indica che il componente è attivo. Il livello di protezione del Firewall è selezionato.

  L'icona di colore rosso indica che l'attività di rete non è filtrata.

- **Antifurto** è lo stato di protezione dei dati in caso di smarrimento o furto del dispositivo (vedere la sezione "Protezione dei dati in caso di smarrimento o furto del dispositivo" a pagina 159).

  L'icona di stato verde indica che la funzione Antifurto è attiva; il nome della funzione è visualizzato solo lo stato del componente.

  L'icona di colore rosso indica che tutte le funzioni di Antifurto sono disabilitate.

- **Protezione privacy** è lo stato di protezione dei dati riservati (vedere la sezione "Mascheramento dei dati personali" a pagina 170).

  L'icona di stato verde indica che il componente è attivo. I dati riservati sono nascosti.

  L'icona di colore giallo avvisa il componente è disabilitato. I dati personali sono visualizzati e accessibili per la visualizzazione.

- **Licenza** è il periodo di validità della licenza (vedere la sezione "Gestione della licenza" a pagina 119).

  L'icona di stato verde indica che il periodo di validità della licenza scadrà tra più di 14 giorni.

  L'icona di stato gialla indica che il periodo di validità della licenza scadrà tra meno di 14 giorni.

L'icona di colore rosso indica che la licenza è scaduta.

Figura 75. Finestra di stato del componente dell'applicazione

È possibile anche accedere alla finestra di stato selezionando **Opzioni** → **Stato di protezione**.

MENU DELL'APPLICAZIONE

I componenti dell'applicazione sono organizzati in gruppi logici e sono accessibili nel menu dell'applicazione. Ogni voce del menu consente di accedere ai parametri del componente selezionato e alla attività di protezione (vedere la figura sotto).

Figura 76. Menu del programma

Il menu di Kaspersky Mobile Security 9.0 contiene le seguenti voci:

- **Anti-Virus**: protezione del file system da virus, scansione manuale e aggiornamento dei database dell'applicazione.
- **Antifurto**: blocco del dispositivo e cancellazione dei dati in caso di smarrimento o furto.
- **Protezione privacy**: mascheramento dei dati riservati sul dispositivo.
- **Criptaggio**: protezione delle informazioni sul dispositivo tramite crittografia.
- **Anti-Spam**: filtro delle chiamate e dei messaggi SMS in entrata indesiderati.
- **Parental Control**: controllo delle chiamate e dei messaggi SMS in uscita.
- **Firewall**: protezione del dispositivo quando è connesso a una rete.
- **Avanzate**: impostazioni generali dell'applicazione, dettagli sull'applicazione, sui database utilizzati e sulla licenza.
- **Stato di protezione**: informazioni sullo stato della protezione del dispositivo.
- **Esci**: uscita dall'applicazione.

➡ *Per aprire il menu dell'applicazione:*

selezionare **Menu**.

Per spostarsi tra le voci del menu dell'applicazione, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

➡ *Per tornare all'applicazione:*

Selezionare **Menu** → **Stato di protezione**.

➡ *Per uscire dall'applicazione:*

Selezionare **Menu** → **Esci**.

PROTEZIONE DEL FILE SYSTEM

Questa sezione fornisce informazioni sul componente Protezione che consente di evitare le infezioni del file system del dispositivo. La sezione spiega inoltre come attivare/arrestare il componente Protezione e regolare le sue impostazioni di funzionamento.

IN QUESTA SEZIONE

Informazioni sul componente Protezione.....127

Abilitazione e disabilitazione del componente Protezione 127

Selezione dell'azione da eseguire sugli oggetti rilevati.....128

INFORMAZIONI SUL COMPONENTE PROTEZIONE

Il componente Protezione viene caricato all'avvio del sistema operativo del dispositivo e rimane residente nella memoria del dispositivo, sottoponendo a scansione tutti i file aperti, salvati o eseguiti. I file vengono sottoposti a scansione mediante il seguente algoritmo:

1. Il componente intercetta ogni tentativo di accesso a qualsiasi file da parte dell'utente o di qualunque programma.

2. Il file viene sottoposto a scansione per verificare la presenza di eventuali oggetti nocivi (malware). Gli oggetti nocivi vengono rilevati mediante confronto con i database dell'applicazione, che contengono le descrizioni di tutti gli oggetti nocivi noti e i metodi per neutralizzarli.

3. Dopo l'analisi, Kaspersky Mobile Security 9.0 può eseguire le seguenti azioni correttive:

   - Se all'interno del file è stato rilevato del codice dannoso, l'applicazione blocca l'accesso al file ed esegue l'azione specificata nelle impostazioni.

   - Se nel file non viene rilevato alcun codice dannoso, il file verrà immediatamente ripristinato.

Le informazioni sui risultati della scansione vengono salvate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

ABILITAZIONE E DISABILITAZIONE DEL COMPONENTE PROTEZIONE

Quando si attiva il componente Protezione, tutte le operazioni eseguite sul sistema sono costantemente sotto controllo. Per assicurare la protezione da oggetti nocivi, vengono utilizzate le risorse del dispositivo. Per ridurre il carico di lavoro sul dispositivo durante l'esecuzione di più attività, è possibile arrestare temporaneamente il componente Protezione.

Gli esperti di Kaspersky Lab consigliano di non disabilitare il componente Protezione, in quanto ciò può causare l'infezione del computer e perdita di dati.

Lo stato corrente del componente Protezione è visualizzato nella finestra **Anti-Virus** accanto alla voce **Protezione**.

È possibile abilitare / disabilitare il componente Protezione nei seguenti modi:

- dal menu delle impostazioni del componente;

- dal menu **Anti-Virus**.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per abilitare il componente Protezione:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Protezione**.

   Verrà aperta la finestra **Impostazioni**.

3. Selezionare la casella **Abilita protezione** (vedere la figura sotto).

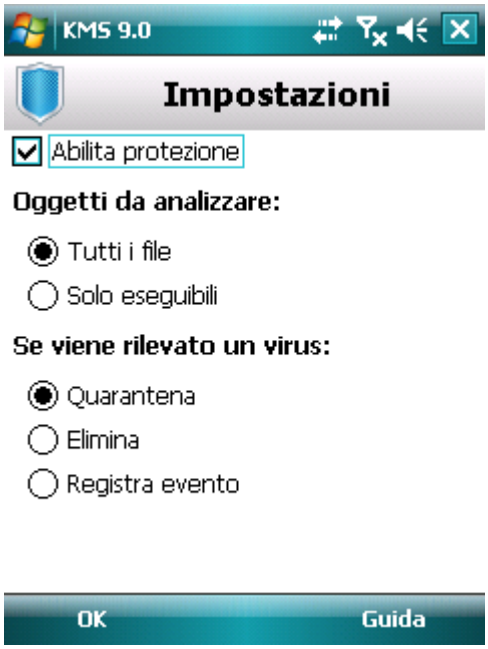


Figura 77. Abilitazione del componente Protezione

4. Premere **OK** per salvare le modifiche.

- *Per disabilitare il componente Protezione:*

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Protezione**.

   Verrà aperta la finestra **Impostazioni**.

3. Deselezionare la casella **Abilita protezione**.

4. Premere **OK** per salvare le modifiche.

- *Per abilitare/ disabilitare rapidamente il componente Protezione:*

1. Selezionare **Menu** → **Anti-Virus**.

2. Verrà aperta la finestra **Anti-Virus**.

3. Premere il pulsante **Abilita** / **Disabilita**. Il nome del pulsante cambia in base allo stato corrente del componente Protezione.

SELEZIONE DELL'AZIONE DA ESEGUIRE SUGLI OGGETTI RILEVATI

Per impostazione predefinita, Kaspersky Mobile Security 9.0 sposta gli oggetti nocivi rilevati in quarantena. È possibile cambiare l'azione che l'applicazione deve eseguire se viene rilevato un oggetto nocivo.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per cambiare i valori delle impostazioni del componente Protezione, assicurarsi che sia attivato.

Per configurare la risposta dell'applicazione quando viene rilevato un oggetto malware:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Protezione**.

   Verrà aperta la finestra **Impostazioni**.

3. Specificare l'azione che l'applicazione deve eseguire se viene rilevato un oggetto nocivo. Per eseguire questa operazione, selezionare un valore per l'impostazione **Se viene rilevato un virus** (vedere la figura sotto):

   - **Quarantena**: mette in quarantena gli oggetti malware.
   - **Elimina**: elimina gli oggetti malware senza avvisare l'utente.
   - **Registra evento**: non elabora gli oggetti malware e registra le informazioni sul loro rilevamento nel report dell'applicazione. Blocca l'oggetto se si tenta di utilizzarlo (ad esempio, per copiarlo o aprirlo).

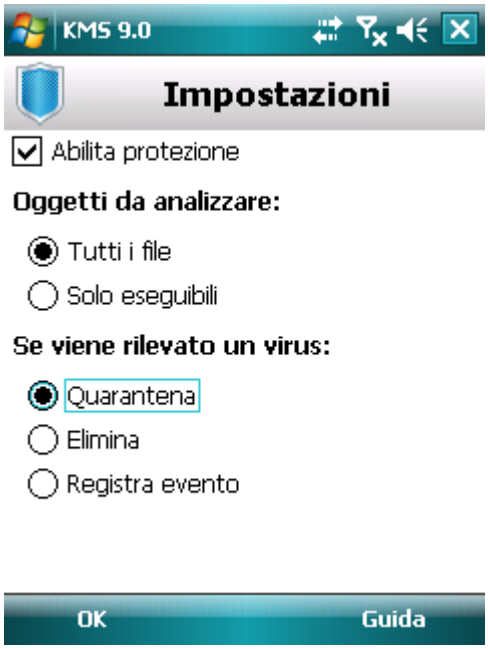


Figura 78. Selezione dell'azione da eseguire sugli oggetti nocivi

4. Premere **OK** per salvare le modifiche.

SCANSIONE DEL DISPOSITIVO

Questa sezione fornisce informazioni sulla scansione anti-virus che consente di rilevare e neutralizzare le minacce nel dispositivo. La sezione specifica inoltre come eseguire l'attività di scansione, come pianificare l'esecuzione delle attività, come selezionare gli oggetti da sottoporre a scansione e come specificare l'azione dell'applicazione su una minaccia rilevata.

IN QUESTA SEZIONE

Informazioni sulle scansioni manuali 130

Avvio di una scansione manuale 130

Avvio di una scansione pianificata 132

Selezione del tipo di oggetti da sottoporre a scansione 133

Configurazione della scansione degli archivi 134

Selezione dell'azione da eseguire sugli oggetti rilevati 135

INFORMAZIONI SULLE SCANSIONI MANUALI

La scansione del dispositivo facilita il rilevamento e la neutralizzazione di eventuali oggetti nocivi. Kaspersky Mobile Security 9.0 consente di eseguire una scansione completa o parziale del dispositivo, ossia solo la scansione del contenuto della memoria integrata del dispositivo o di una cartella specifica (incluse le cartelle presenti nella scheda di memoria).

La procedura di scansione del dispositivo è la seguente:

1. Kaspersky Mobile Security 9.0 esegue la scansione dei tipi di file selezionati (vedere la sezione "Selezione dei tipi di oggetti da sottoporre a scansione" a pagina 133).

2. Ogni file viene sottoposto a scansione per verificare la presenza di eventuali oggetti nocivi (malware). Gli oggetti nocivi vengono rilevati mediante confronto con i database dell'applicazione, che contengono le descrizioni di tutti gli oggetti nocivi noti e i metodi per neutralizzarli.

   Dopo l'analisi, Kaspersky Mobile Security 9.0 può eseguire le seguenti azioni correttive:

   - Se all'interno del file è stato rilevato del codice dannoso, Kaspersky Mobile Security 9.0 blocca l'accesso al file ed esegue l'azione specificata nelle impostazioni (vedere la sezione "Selezione delle azioni da eseguire sugli oggetti" a pagina 135).

   - Se non viene rilevato alcun codice dannoso, il file diventa immediatamente accessibile per l'uso.

Un'attività di scansione può essere avviata manualmente o automaticamente in base a una pianificazione definita precedentemente (vedere la sezione "Avvio di una scansione pianificata" a pagina 132).

Le informazioni sui risultati della scansione manuale vengono salvate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

AVVIO DI UNA SCANSIONE MANUALE

È possibile avviare una scansione manualmente in qualsiasi momento. Il momento migliore è tuttavia quando il processore del dispositivo non è occupato ad eseguire altre operazioni.

Per avviare manualmente una scansione anti-virus:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

   Verrà aperta la finestra **Scansione**.

3. Selezionare l'area di scansione del dispositivo (vedere la figura sotto):

   - **Scansione completa**: esegue la scansione dell'intero file system del dispositivo. Per impostazione predefinita, vengono sottoposti a scansione i seguenti oggetti: memoria del dispositivo e scheda di memoria.

   - **Scansione memoria**: esegue la scansione dei processi avviati nella memoria di sistema e dei file corrispondenti.

   - **Scansione cartella**: esegue la scansione di un determinato oggetto nel file system del dispositivo o sulla scheda di memoria. Se si seleziona **Scansione cartella**, verrà aperta una finestra che visualizza il file system del dispositivo. Utilizzare i pulsanti di spostamento per spostarsi nel file system. Per avviare la scansione della cartella, selezionare la cartella desiderata e selezionare **Scansione**.

Figura 79. Selezione dell'area di scansione

All'avvio della scansione, si aprirà la finestra del processo di scansione che visualizza lo stato della scansione (vedere la figura sotto), incluso il numero di oggetti sottoposti a scansione, il percorso dell'oggetto sottoposto a scansione e un indicatore che fornisce la percentuale di completamento della scansione.

Figura 80. Finestra di scansione

Se Kaspersky Mobile Security 9.0 rileva un oggetto infetto, esegue un'azione in base ai parametri di scansione impostati (vedere la sezione "Selezione di un'azione da eseguire sugli oggetti" a pagina 135).

Per impostazione predefinita, se Kaspersky Mobile Security 9.0 rileva una minaccia, la mette in quarantena.

Al termine della scansione, sullo schermo vengono visualizzate statistiche complessive con le seguenti informazioni:

- numero di oggetti sottoposti a scansione;
- numero di virus rilevati, messi in quarantena o eliminati;
- numero di oggetti ignorati (ad esempio, file bloccati dal sistema operativo o file non eseguibili, durante la scansione dei soli file di programma eseguibili);
- ora della scansione.

4. Al completamento dell'operazione, premere **OK**.

AVVIO DI UNA SCANSIONE PIANIFICATA

Kaspersky Mobile Security consente di creare una pianificazione di ore in cui le scansioni verranno avviate automaticamente. Le scansioni vengono eseguite in background. Quando viene rilevato un oggetto infetto, su di esso verrà eseguita l'azione selezionata nelle impostazioni di scansione (vedere la sezione "Selezione di un'azione da eseguire sugli oggetti" a pagina 135).

Per impostazione predefinita, le impostazioni pianificate sono disabilitate.

➡ *Per configurare una scansione pianificata:*

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

   Verrà aperta la finestra **Scansione**.

3. Selezionare l'opzione **Pianifica scansione**.

   Verrà aperta la finestra **Pianifica**.

4. Selezionare la casella **Scansione pianificata** (vedere la figura sotto).

5. Selezionare uno dei valori per l'impostazione **Frequenza**:

   - **Giornaliero**: esegue la scansione ogni giorno. Specificare l'**Ora** nel campo di immissione per impostare l'ora del giorno in cui verrà avviata la scansione.

   - **Settimanale**: esegue la scansione una volta alla settimana. Specificare l'**Ora** e il **Giorno della settimana**.

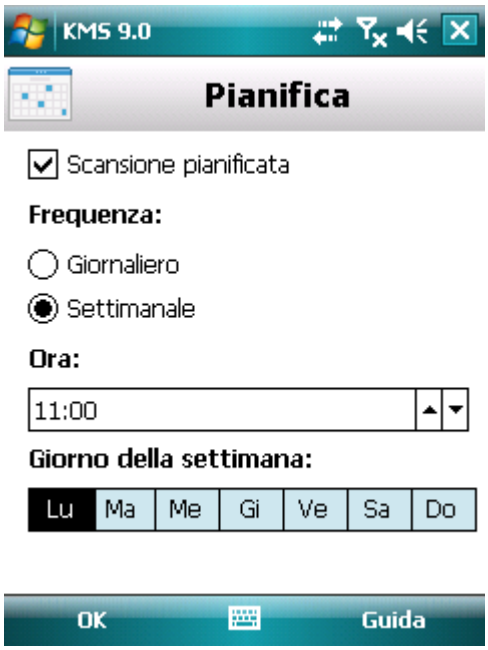


Figura 81. Configurazione di una scansione automatica pianificata

6. Premere **OK** per salvare le modifiche.

SELEZIONE DEL TIPO DI OGGETTI DA SOTTOPORRE A SCANSIONE

È possibile specificare il tipo di oggetti da sottoporre a scansione per rilevare codice dannoso.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per selezionare gli oggetti da sottoporre a scansione:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

   Verrà aperta la finestra **Scansione**.

3. Selezionare l'opzione **Oggetti e azioni**.

   Verrà aperta la finestra **Oggetti e azioni**.

4. Selezionare gli oggetti da sottoporre a scansione nella sezione **Oggetti da analizzare** (vedere la figura sotto).

   - **Tutti i file**: esegue la scansione di tutti i tipi di file. Vengono sottoposti a scansione gli archivi nei seguenti formati: *.zip, *.sis, *.cab e *.sisx.

   - **Solo eseguibili**: esegue solo la scansione dei file di programma dei seguenti formati: *.exe, *.dll, *.sis, *.mdl, *.app, *.rdl, *.prt, *.pxt, *.ldd, *.pdd, *.class. Inoltre, gli archivi non vengono decompressi e sottoposti a scansione.

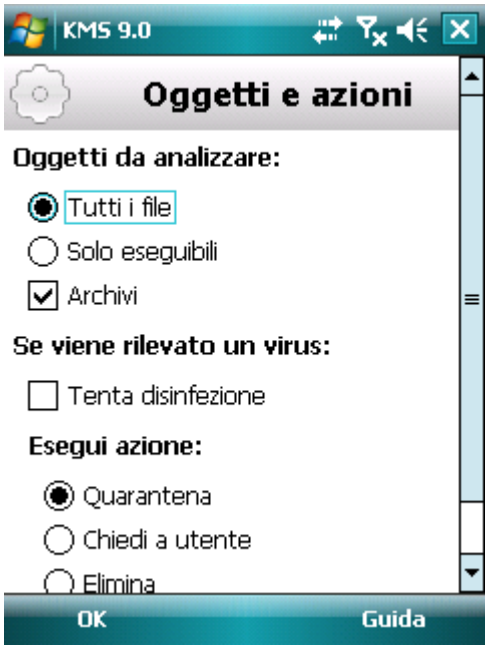


Figura 82. Selezione degli oggetti da sottoporre a scansione

5. Premere **OK** per salvare le modifiche.

CONFIGURAZIONE DELLA SCANSIONE DEGLI ARCHIVI

I virus si nascondono spesso negli archivi. Per eseguire la scansione del contenuto degli archivi, è necessario decomprimerli. Ciò può ridurre in modo significativo la velocità di scansione del dispositivo.

Per impostazione predefinita, la decompressione degli archivi è abilitata. L'applicazione esegue la scansione degli archivi nei seguenti formati: *.zip, *.sis, *.cab e *.sisx. Per aumentare la velocità della scansione è possibile disabilitare la decompressione degli archivi.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

➡ *Per disabilitare la decompressione degli archivi:*

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

   Verrà aperta la finestra **Scansione**.

3. Selezionare l'opzione **Oggetti e azioni**.

   Verrà aperta la finestra **Oggetti e azioni**.

4. Deselezionare la casella **Archivi** nella sezione **Oggetti da analizzare**.

5. Premere **OK** per salvare le modifiche.

SELEZIONE DELL'AZIONE DA ESEGUIRE SUGLI OGGETTI RILEVATI

Per impostazione predefinita, Kaspersky Mobile Security 9.0 sposta gli oggetti infetti rilevati in quarantena. È possibile cambiare le azioni che l'applicazione eseguirà quando rileva un oggetto nocivo.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per configurare la risposta dell'applicazione quando viene rilevato un oggetto malware:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Scansione**.

   Verrà aperta la finestra **Scansione**.

3. Selezionare l'opzione **Oggetti e azioni**.

   Verrà aperta la finestra **Oggetti e azioni**.

4. Se si desidera che l'applicazione tenti di disinfettare gli oggetti infetti, selezionare la casella **Tenta disinfezione** accanto all'impostazione **Se viene rilevato un virus**.

5. Specificare l'azione da eseguire nei confronti di un oggetto nocivo rilevato. Per eseguire questa operazione, selezionare un valore per l'impostazione **Esegui azione**:

   Se in precedenza è stata selezionata la casella **Tenta disinfezione**, il nome di questa impostazione cambia in **Se fallisce disinfezione**. Questa impostazione determina l'azione del programma, anche se la correzione dell'oggetto non va a buon fine.

   - **Quarantena**: mette in quarantena gli oggetti.
   - **Chiedi a utente**: richiede all'utente quale azione eseguire quando viene rilevato un oggetto nocivo.
   - **Elimina**: elimina gli oggetti malware senza avvisare l'utente.

- **Registra evento**: non elabora gli oggetti malware e registra le informazioni sul loro rilevamento nel report dell'applicazione. Blocca l'oggetto se si tenta di utilizzarlo (ad esempio, per copiarlo o aprirlo).

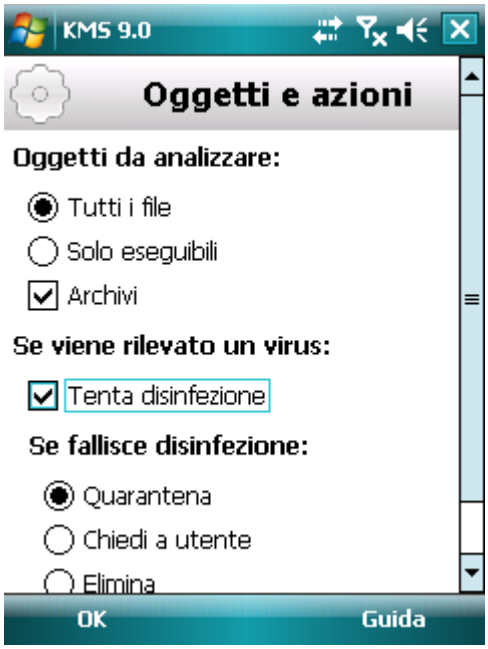


Figura 83. Selezione dell'azione da eseguire sugli oggetti nocivi

6. Premere **OK** per salvare le modifiche.

QUARANTENA DEGLI OGGETTI MALWARE

Questa sezione fornisce informazioni sulla *quarantena*, una cartella speciale in cui vengono collocati gli oggetti potenzialmente nocivi. La sezione specifica inoltre come gestire gli oggetti in quarantena: come visualizzare, ripristinare o eliminare gli oggetti presenti in questa cartella.

IN QUESTA SEZIONE

Informazioni sulla Quarantena....136

Visualizzazione di oggetti in quarantena....137

Ripristino di oggetti dalla quarantena....137

Eliminazione di oggetti dalla quarantena....138

INFORMAZIONI SULLA QUARANTENA

La Quarantena è una cartella specifica in cui Kaspersky Mobile Security 9.0 colloca gli oggetti potenzialmente nocivi.

Gli oggetti nocivi possono essere rilevati e messi in quarantena durante una scansione del dispositivo oppure durante il funzionamento di Protezione.

Gli oggetti messi in quarantena vengono memorizzati in un formato compresso che ne impedisce l'attivazione e neutralizza la potenziale minaccia al dispositivo. Gli oggetti messi in quarantena possono essere eliminati o ripristinati dall'utente.

VISUALIZZAZIONE DI OGGETTI IN QUARANTENA

È possibile visualizzare gli oggetti messi in quarantena. Per ogni oggetto vengono specificati il nome completo e la data di rilevamento.

Per visualizzare l'elenco degli oggetti in quarantena:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Quarantena**.

   Verrà aperta la finestra **Quarantena** contenente un elenco degli oggetti memorizzati nella Quarantena (vedere la figura sotto).

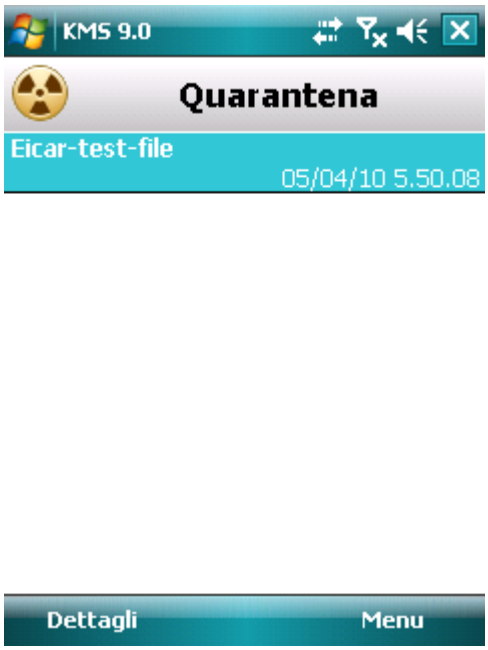


Figura 84. Elenco di oggetti in quarantena

RIPRISTINO DI OGGETTI DALLA QUARANTENA

Se si è sicuri che l'oggetto rilevato non rappresenta una minaccia per il dispositivo, è possibile ripristinarlo dalla quarantena. L'oggetto ripristinato viene rimesso nella cartella originale.

Per ripristinare un oggetto dalla quarantena:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Quarantena**.

   Verrà aperta la finestra **Quarantena**.

3. Selezionare l'oggetto che si desidera ripristinare e premere **Menu** → **Ripristina**.

L'oggetto selezionato verrà ripristinato dalla quarantena nella cartella originale.

ELIMINAZIONE DI OGGETTI DALLA QUARANTENA

È possibile eliminare uno o tutti gli oggetti memorizzati nella quarantena.

- *Per eliminare un oggetto dalla quarantena:*

  1. Selezionare **Menu** → **Anti-Virus**.

     Verrà aperta la finestra **Anti-Virus**.

  2. Selezionare l'opzione **Quarantena**.

     Verrà aperta la finestra **Quarantena**.

  3. Selezionare l'oggetto da eliminare e premere **Menu**→ **Elimina**.

L'oggetto selezionato verrà eliminato dalla quarantena.

- *Per eliminare tutti gli oggetti in quarantena:*

  1. Selezionare **Menu** → **Anti-Virus**.

     Verrà aperta la finestra **Anti-Virus**.

  2. Selezionare l'opzione **Quarantena**.

     Verrà aperta la finestra **Quarantena**.

  3. Premere **Menu** → **Elimina tutto**.

Tutti gli oggetti in quarantena verranno eliminati.

FILTRO DELLE CHIAMATE E DEI MESSAGGI SMS IN ENTRATA

Questa sezione fornisce informazioni sul componente Anti-Spam che filtra i messaggi e le chiamate in entrata in base alla Lista bloccati e alla Lista consentiti. La sezione specifica inoltre come creare la Lista bloccati e la Lista consentiti, come selezionare un'azione di Anti-Spam nei confronti dei messaggi e delle chiamate in entrata e come configurare le impostazioni di funzionamento del componente.

IN QUESTA SEZIONE

Informazioni su Anti-Spam 139

Modalità Anti-Spam 140

Modifica della modalità Anti-Spam 140

Creazione di una Lista bloccati 141

Creazione di una Lista consentiti 144

Risposta ai messaggi SMS e alle chiamate da contatti non in rubrica 147

Risposta ai messaggi SMS da mittenti non numerici 148

Selezione di una risposta ai messaggi SMS in entrata 149

Selezione di una risposta alle chiamate in entrata 150

INFORMAZIONI SU ANTI-SPAM

Anti-Spam protegge il dispositivo dalla ricezione di chiamate e messaggi indesiderati. Anti-Spam filtra i messaggi SMS e le chiamate in entrata utilizzando la Lista bloccati e la Lista consentiti.

Le liste sono composte da voci. Ogni voce può contenere le seguenti impostazioni:

- tipo di dati (messaggio SMS, chiamate, messaggio SMS e chiamate) cui si applicano le impostazioni di filtro (impostazione obbligatoria);
- numero dell'abbonato da cui vengono ricevuti i dati;
- testo contenuto in un messaggio SMS.

Anti-Spam filtra i messaggi SMS e le chiamate in base alle impostazioni selezionate (vedere la sezione "Modalità Anti-Spam" a pagina 140). In base a queste impostazioni, Anti-Spam esegue la scansione di ogni messaggio SMS o chiamata in entrata e determina se il messaggio o la chiamata è desiderata o indesiderata (spam). Non appena Anti-Spam assegna lo stato di desiderato o indesiderato a un messaggio SMS o a una chiamata, la scansione termina.

Per impostazione predefinita, l'algoritmo di Anti-Spam è composto dai seguenti passaggi:

1. Scansione dei messaggi SMS in entrata per verificare se sono identici al numero dell'abbonato e al testo:
   a. Dalla Lista bloccati. Se nella lista viene trovata una voce in cui il numero e il testo sono identici ai dati del messaggio SMS in entrata, il messaggio SMS viene considerato come indesiderato e bloccato. Il programma elimina il messaggio SMS bloccato.
   b. Dalla Lista consentiti. Se nella lista viene trovata una voce in cui il numero e il testo sono identici ai dati del messaggio SMS in entrata, il messaggio SMS viene considerato come desiderato e consentito.
2. Scansione delle chiamate e dei messaggi SMS per verificare la conformità solo rispetto al numero:
   a. Dalla Lista bloccati. Se nella lista viene trovata una voce in cui il numero è identico al numero del mittente (mentre il testo non è stato specificato nella voce), la chiamata o il messaggio SMS viene considerato come spam e bloccato. Il programma elimina il messaggio SMS bloccato.
   b. Dalla Lista consentiti. Se nella lista viene trovata una voce in cui il numero è identico al numero del mittente (mentre il testo non è stato specificato nella voce), la chiamata o il messaggio SMS viene considerato come desiderato e consentito.

3. Scansione dei messaggi per verificare la conformità solo rispetto al testo:

   a. Dalla Lista bloccati. Se nella lista viene trovata una voce in cui il testo è identico ai dati del messaggio SMS in entrata (mentre il numero non è stato specificato nella voce), il messaggio SMS viene considerato come spam e bloccato. Il programma elimina il messaggio SMS bloccato.

   b. Dalla Lista consentiti. Se nella lista viene trovata una voce in cui il testo è identico ai dati del messaggio SMS in entrata (mentre il numero non è stato specificato nella voce), il messaggio SMS viene considerato come desiderato e consentito.

4. Selezione di un'azione. Se non viene trovata alcuna conformità nella Lista bloccati o nella Lista consentiti, per impostazione predefinita Anti-Spam recapita le chiamate e i messaggi SMS e suggerisce di eseguire un'azione nei confronti delle chiamate o dei messaggi nella finestra di notifica. È possibile inoltre visualizzare informazioni aggiuntive nella notifica. Per le chiamate ricevute viene indicato il numero del chiamante. Per i messaggi SMS vengono visualizzati il numero dell'abbonato e il contenuto.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

MODALITÀ ANTI-SPAM

Per modalità Anti-Spam si intende una configurazione di base, o una raccolta di parametri, del componente che protegge il dispositivo da chiamate e messaggi indesiderati.

Sono disponibili le seguenti modalità Anti-Spam:

- **Disabilitato**: tutti i messaggi SMS e le chiamate vengono consentiti. Disabilita Anti-Spam.
- **Lista consentiti**: i messaggi SMS e le chiamate corrispondenti alle voci nella Lista consentiti vengono consentiti. Tutti gli altri messaggi SMS e le chiamate verranno bloccati. I messaggi SMS bloccati vengono eliminati.
- **Lista bloccati**: i messaggi SMS e le chiamate corrispondenti alle voci nella Lista bloccati vengono bloccati. I messaggi SMS bloccati vengono eliminati. Tutti gli altri messaggi SMS e le chiamate verranno bloccati.
- **Entrambe le liste**: i messaggi SMS e le chiamate in entrata vengono filtrati utilizzando entrambe la Lista bloccati e la Lista consentiti. Se viene ricevuto un messaggio SMS o una chiamata da un numero di telefono non trovato su nessuna delle due liste, Anti-Spam invierà una notifica all'utente e informerà di bloccare o ricevere il messaggio SMS o la chiamata e di aggiungere questo numero di telefono alla Lista consentiti o alla Lista bloccati. Questa è la modalità predefinita.

È possibile modificare la modalità Anti-spam (vedere la sezione "Modifica della modalità Anti-Spam" a pagina 140). La modalità corrente di Anti-Spam è visualizzata nella finestra **Anti-Spam** accanto alla voce del menu **Modalità**.

MODIFICA DELLA MODALITÀ ANTI-SPAM

Per selezionare la modalità di funzionamento di Anti-Spam:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **Modalità**.

3. Selezionare un valore per l'impostazione **Modalità Anti-Spam** (vedere la figura sotto).

Figura 85. Modifica della modalità Anti-Spam

4. Premere **OK** per salvare le modifiche.

CREAZIONE DI UNA LISTA BLOCCATI

È possibile creare una Lista bloccati in base alla quale Anti-Spam blocca le chiamate e i messaggi SMS in entrata.

La lista contiene numeri di telefono e frasi la cui presenza in un messaggio SMS indica che si tratta di spam.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

IN QUESTA SEZIONE

Aggiunta di voci alla Lista bloccati 141

Modifica di voci nella Lista bloccati 143

Eliminazione di voci dalla Lista bloccati 144

AGGIUNTA DI VOCI ALLA LISTA BLOCCATI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri Anti-Spam. Se un numero è già stato salvato in una di queste liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

➡ *Per aggiungere una voce alla Lista bloccati di Anti-Spam:*

1. Selezionare **Menu** → **Anti-Spam**.

Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.

3. Selezionare **Menu** → **Aggiungi** (vedere la figura sotto).

   Verrà aperta la finestra **Aggiungi voce**.

Figura 86. Aggiunta di voci alla Lista bloccati

4. Selezionare i valori per le seguenti impostazioni (vedere la figura sotto).

   - **Blocca in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà bloccato da Anti-Spam:
     - **Chiamate e SMS**: blocca le chiamate e i messaggi SMS in entrata.
     - **Solo chiamate**: blocca solo le chiamate in entrata.
     - **Solo SMS**: blocca solo i messaggi SMS in entrata.
   - **Numero di telefono**: numero di telefono da cui le chiamate e/o i messaggi SMS ricevuti vengono consentiti. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS è spam. L'impostazione è disponibile se per l'impostazione **Blocca in entrata** è impostato il valore **Solo SMS**.

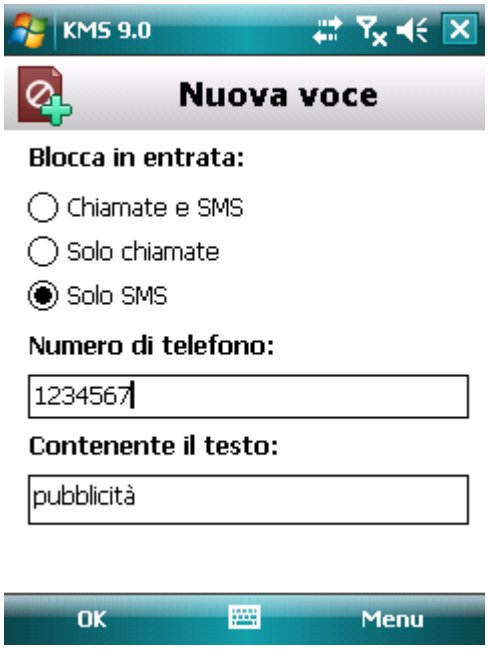


Figura 87. Impostazioni della voce

5. Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA BLOCCATI

È possibile cambiare il valore di tutte le impostazioni relative ai numeri presenti nella Lista bloccati.

Per modificare una voce della Lista bloccati di Anti-Spam:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.

3. Selezionare dalla lista la voce che si desidera modificare e selezionare **Menu** → **Modifica**.

   Verrà aperta la finestra **Modifica voce**.

4. Modificare le impostazioni necessarie:

   - **Blocca in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà bloccato da Anti-Spam:

     - **Chiamate e SMS**: blocca le chiamate e i messaggi SMS in entrata.

     - **Solo chiamate**: blocca solo le chiamate in entrata.

     - **Solo SMS**: blocca solo i messaggi SMS in entrata.

   - **Numero di telefono**: numero di telefono da cui le chiamate e/o i messaggi SMS ricevuti vengono consentiti. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra,

una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS è spam. L'impostazione è disponibile se per l'impostazione **Blocca in entrata** è impostato il valore **Solo SMS**.

5. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA BLOCCATI

In caso di aggiunta accidentale di un numero alla Lista bloccati è possibile eliminare tale numero dalla lista. È possibile inoltre svuotare la Lista bloccati di Anti-Spam rimuovendo da essa tutte le voci.

Per eliminare una voce dalla Lista bloccati di Anti-Spam:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.

3. Selezionare dalla lista la voce da eliminare e selezionare **Menu** → **Elimina**.

4. Confermare la cancellazione della voce premendo il pulsante **OK**.

Per svuotare la Lista bloccati:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.

3. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

CREAZIONE DI UNA LISTA CONSENTITI

È possibile creare una Lista consentiti in base alla quale Anti-Spam consente le chiamate e i messaggi SMS in entrata.

La lista contiene i numeri di telefono dei mittenti e le frasi che non si considerano come spam.

IN QUESTA SEZIONE

Aggiunta di voci alla Lista consentiti 145

Modifica di voci nella Lista consentiti 146

Eliminazione di voci dalla Lista consentiti 147

AGGIUNTA DI VOCI ALLA LISTA CONSENTITI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri Anti-Spam. Se un numero è già stato salvato in una di queste liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

Per aggiungere una voce alla Lista consentiti di Anti-Spam:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

3. Selezionare **Menu** → **Aggiungi** (vedere la figura sotto).

   Verrà aperta la finestra **Aggiungi voce**.

Figura 88. Aggiunta di voci alla Lista consentiti

4. Selezionare i valori per le seguenti impostazioni (vedere la figura sotto).

   - **Consenti in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà consentito da Anti-Spam:
     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in entrata.
     - **Solo chiamate**: consente solo le chiamate in entrata.
     - **Solo SMS**: consente solo i messaggi SMS in entrata.
   - **Numero di telefono**: numero di telefono per il quale la ricezione di messaggi SMS e/o di chiamate viene consentita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS non è spam. L'impostazione è disponibile se per l'impostazione **Consenti in entrata** è impostato il valore **Solo SMS**.

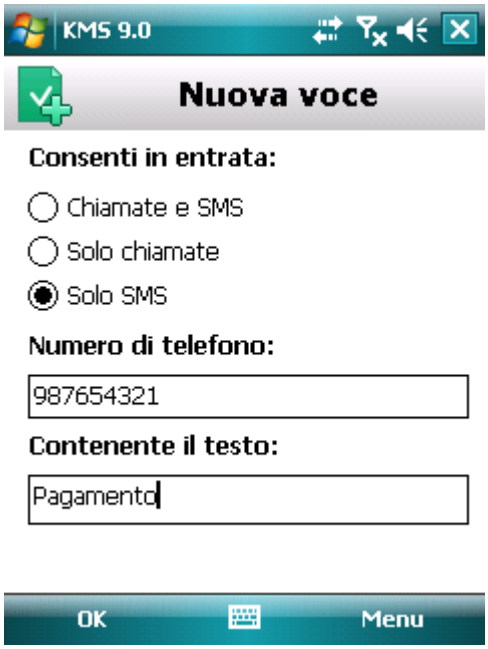


Figura 89. Impostazioni della voce

5. Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA CONSENTITI

È possibile cambiare i valori di tutte le impostazioni relative ai numeri presenti nella Lista consentiti.

➧ *Per modificare una voce della Lista consentiti di Anti-Spam:*

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

3. Selezionare dalla lista la voce che si desidera modificare e selezionare **Menu** → **Modifica**.

   Verrà aperta la finestra **Modifica voce**.

4. Modificare le impostazioni necessarie:

   - **Consenti in entrata**: tipo di informazione in entrata da un numero di abbonato che verrà consentito da Anti-Spam:

     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in entrata.

     - **Solo chiamate**: consente solo le chiamate in entrata.

     - **Solo SMS**: consente solo i messaggi SMS in entrata.

   - **Numero di telefono**: numero di telefono per il quale la ricezione di messaggi SMS e/o di chiamate viene consentita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra,

una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

- **Contenente il testo**: parole chiave/frasi che indicano che il messaggio SMS non è spam. L'impostazione è disponibile se per l'impostazione **Consenti in entrata** è impostato il valore **Solo SMS**.

5. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA CONSENTITI

È possibile rimuovere una voce o svuotare completamente la Lista consentiti.

Per eliminare una voce dalla Lista consentiti di Anti-Spam:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

3. Selezionare dalla lista la voce da eliminare e selezionare **Menu** → **Elimina**.

4. Confermare la cancellazione della voce premendo il pulsante **OK**.

Per svuotare la Lista consentiti:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Lista consentiti**.

   Verrà aperta la finestra **Lista consentiti**.

3. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

RISPOSTA AI MESSAGGI SMS E ALLE CHIAMATE DA CONTATTI NON IN RUBRICA

Se è selezionata la modalità Anti-Spam **Entrambe le liste** o **Lista consentiti** (vedere la sezione "Modalità Anti-Spam" a pagina 140), è possibile specificare una risposta di Anti-Spam verso i messaggi SMS e le chiamate provenienti da abbonati i cui numeri non sono contenuti nella rubrica. Inoltre, Anti-Spam consente di espandere la Lista consentiti aggiungendovi i numeri dall'elenco dei contatti.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per selezionare la risposta di Anti-Spam verso un numero non incluso nella rubrica:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Modalità**.

3. Verrà aperta la finestra **Modalità**.

4. Selezionare il valore richiesto per l'impostazione **Consenti contatti** (vedere la figura sotto):

   - se si desidera che Anti-Spam consideri i numeri della rubrica come Lista consentiti aggiuntiva e blocchi la ricezione dei messaggi SMS e delle chiamate da mittenti non presenti nella rubrica, selezionare la casella **Consenti contatti**;

   - se si desidera che Anti-Spam filtri i messaggi SMS e le chiamate solo in base alla modalità Anti-Spam impostata, deselezionare la casella **Consenti contatti**.

Figura 90. Risposta di Anti-Spam verso i numeri non inclusi nella rubrica del dispositivo

5. Premere **OK** per salvare le modifiche.

RISPOSTA AI MESSAGGI SMS DA MITTENTI NON NUMERICI

Se è selezionata la modalità Anti-Spam **Entrambe le liste** o **Lista bloccati** (vedere la sezione "Modifica della modalità Anti-Spam" a pagina 140), è possibile espandere ulteriormente la Lista bloccati aggiungendovi contatti non numerici (incluse le lettere). Anti-Spam bloccherà quindi i messaggi SMS provenienti dai mittenti non numerici.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per impostare la risposta di Anti-Spam alla ricezione di messaggi da mittenti non numerici:

1. Selezionare **Menu** → **Anti-Spam**.

   Verrà aperta la finestra **Anti-Spam**.

2. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **Modalità**.

3. Selezionare un valore per l'impostazione **Blocca mittenti non numerici** (vedere la figura sotto):

   - per far sì che Anti-Spam elimini automaticamente i messaggi dai mittenti non numerici, selezionare la casella **Blocca mittenti non numerici**;

- se si desidera che Anti-Spam filtri i messaggi SMS e le chiamate da mittenti non numerici solo in base alla modalità Anti-Spam impostata, deselezionare la casella **Blocca mittenti non numerici**.

Figura 91. Configurazione dell'azione di Anti-Spam alla ricezione di messaggi SMS da mittenti non numerici

4. Premere **OK** per salvare le modifiche.

SELEZIONE DI UNA RISPOSTA AI MESSAGGI SMS IN ENTRATA

Per impostazione predefinita, la modalità Anti-Spam impostata è **Entrambe le liste** (vedere la sezione "Modalità Anti-Spam" a pagina 140). Anti-Spam esegue la scansione dei messaggi SMS in entrata in base alla Lista consentiti e alla Lista bloccati.

Se il numero del mittente non è contenuto né nella Lista bloccati né nella Lista consentiti, Anti-Spam informerà l'utente e richiederà di selezionare una delle azioni suggerite nei confronti del messaggio SMS (vedere la figura sotto).

Figura 92. Notifica di Anti-Spam alla ricezione di un messaggio SMS

Utilizzando il menu, è possibile selezionare una delle seguenti azioni da eseguire nei confronti del messaggio:

- Per bloccare il messaggio SMS e aggiungere il numero di telefono del mittente alla Lista bloccati, selezionare **Menu → Aggiungi a Lista bloccati**.
- Per recapitare il messaggio SMS e aggiungere il numero di telefono del mittente alla Lista consentiti, selezionare **Menu → Aggiungi a Lista consentiti**.
- Per recapitare il messaggio SMS senza aggiungere il numero di telefono del mittente a nessuna delle liste, premere **Ignora**.

Le informazioni su messaggi bloccati vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

SELEZIONE DI UNA RISPOSTA ALLE CHIAMATE IN ENTRATA

Per impostazione predefinita, la modalità Anti-Spam impostata è **Entrambe le liste** (vedere la sezione "Modalità Anti-Spam" a pagina 140). Anti-Spam esegue la scansione delle chiamate in entrata in base alla Lista consentiti e alla Lista consentiti.

Se il numero del mittente non è contenuto né nella Lista bloccati né nella Lista consentiti, Anti-Spam informerà l'utente dopo aver completato la scansione e richiederà un'azione nei confronti della chiamata in entrata (vedere la figura sotto).

Figura 93. Notifica di Anti-Spam all'accettazione della chiamata

È possibile selezionare una delle seguenti azioni da eseguire per il numero da cui è stata effettuata la chiamata:

- Per aggiungere il numero di telefono del chiamante alla Lista bloccati, selezionare **Menu → Aggiungi a Lista bloccati**.
- Per aggiungere il numero di telefono del chiamante alla Lista consentiti, selezionare **Menu → Aggiungi a Lista consentiti**.
- **Ignora**: non aggiunge il numero del chiamante a nessuna delle liste.

Le informazioni sulle chiamate bloccate vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 102).

LIMITAZIONE DELLE CHIAMATE E DEI MESSAGGI SMS IN USCITA. PARENTAL CONTROL

Questa sezione fornisce informazioni sul componente Parental Control, che consente di limitare le chiamate e i messaggi SMS in uscita verso numeri definiti. La sezione spiega inoltre come creare una lista di numeri consentiti e bloccati e come specificare le impostazioni di Parental control .

IN QUESTA SEZIONE

Informazioni su Parental Control 152

Modalità Parental Control 152

Abilitazione/disabilitazione di Parental Control 152

Creazione di una Lista bloccati..... 153

Creazione di una Lista consentiti..... 156

INFORMAZIONI SU PARENTAL CONTROL

Il componente Parental Control filtra i messaggi SMS e le chiamate in uscita utilizzando la Lista bloccati e la Lista consentiti.

Il filtro funziona nello stesso modo descritto in precedenza per il componente Anti-Spam: i messaggi SMS e le chiamate corrispondenti a una voce nella Lista bloccati vengono bloccati, mentre sono consentiti se corrispondono a una voce nella Lista consentiti.

Parental Control blocca i messaggi SMS inviati utilizzando solo le funzioni standard del dispositivo. I messaggi SMS inviati con applicazioni di terze parti non vengono bloccati.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

MODALITÀ PARENTAL CONTROL

Per modalità Parental Control si intende una configurazione di base, o una raccolta di parametri, del componente che consente a un genitore di limitare la possibilità di inviare messaggi ed effettuare chiamate indesiderate da parte di un figlio.

Sono disponibili le seguenti modalità Parental Control :

- **Disabilitato**: disabilita Parental Control . Non filtra i messaggi SMS e le chiamate in uscita.

  Questa è la modalità predefinita selezionata

- **Lista consentiti**: consente l'invio di messaggi SMS e/o di effettuare chiamate solo ai numeri inclusi nella Lista consentiti (vedere la sezione "Creazione di una Lista consentiti" a pagina 156). Tutti gli altri messaggi e le chiamate verranno bloccati.

- **Lista bloccati**: blocca l'invio di messaggi SMS e/o di chiamate solo ai numeri inclusi nella Lista bloccati (vedere la sezione "Creazione di una Lista bloccati" a pagina 153). Tutti gli altri messaggi e le chiamate verranno consentiti.

È possibile modificare la modalità Parental Control (vedere la sezione "Abilitazione/disabilitazione di Parental Control " a pagina 152). La modalità di funzionamento corrente di Parental Control è visualizzata nella finestra **Parental Control** accanto alla voce **Modalità**.

ABILITAZIONE/DISABILITAZIONE DI PARENTAL CONTROL

➧ *Per modificare la modalità Parental Control :*

1. Selezionare **Menu** → **Parental Control**.

2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **Modalità**.
4. Selezionare una delle modalità Parental Control suggerita (vedere la figura sotto).

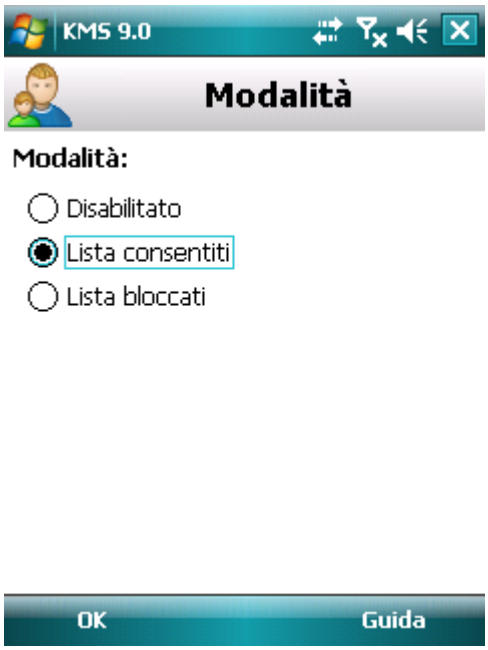


Figura 94. Modifica della modalità Parental Control

5. Premere **OK** per salvare le modifiche.

CREAZIONE DI UNA LISTA BLOCCATI

È possibile creare una Lista bloccati in base alla quale Parental Control blocca i messaggi SMS e le chiamate in uscita. La lista contiene i numeri di telefono per i quali l'invio di messaggi SMS e l'effettuazione di chiamate non è bloccato.

Le informazioni sulle chiamate e sui messaggi SMS bloccati vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

IN QUESTA SEZIONE

Aggiunta di voci alla Lista bloccati 153

Modifica di voci nella Lista bloccati 155

Eliminazione di voci dalla Lista bloccati 156

AGGIUNTA DI VOCI ALLA LISTA BLOCCATI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri di Parental Control . Se un numero è già stato salvato in una delle liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

Per aggiungere una voce alla Lista bloccati di Parental Control :

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.
4. Selezionare **Menu** → **Aggiungi** (vedere la figura sotto).

Figura 95. Aggiunta di voci alla Lista bloccati

Verrà aperta la finestra **Aggiungi voce**.

5. Selezionare i valori per le seguenti impostazioni (vedere la figura sotto).

   - **Blocca in uscita**: tipo di informazione in uscita da un numero di abbonato che verrà bloccato da Parental Control :
     - **Chiamate e SMS**: blocca le chiamate e i messaggi SMS in uscita.
     - **Solo chiamate**: blocca solo le chiamate in uscita.
     - **Solo SMS**: blocca solo i messaggi SMS in uscita.

- **Numero di telefono**: numero di telefono che verrà bloccato per i messaggi SMS e/o le chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

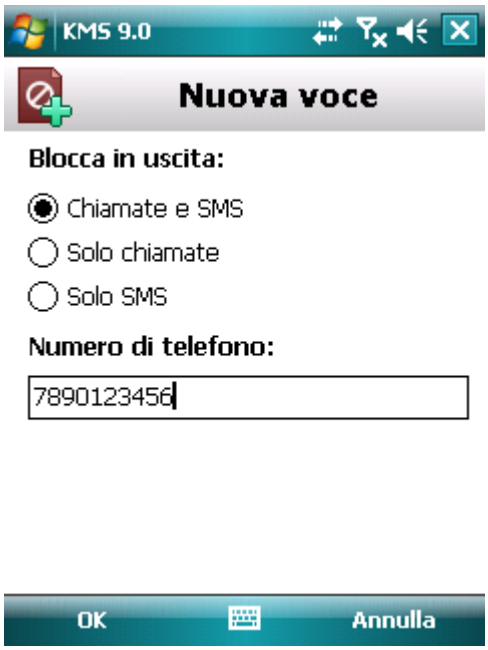


Figura 96. Impostazioni della voce

6. Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA BLOCCATI

È possibile cambiare il valore di tutte le impostazioni relative ai numeri presenti nella Lista bloccati.

Per modificare una voce della Lista bloccati di Parental Control :

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.
4. Selezionare dalla lista la voce che si desidera modificare e selezionare **Menu** → **Modifica**.

   Verrà aperta la finestra **Modifica voce**.
5. Modificare le impostazioni necessarie:

   - **Blocca in uscita**: tipo di informazione in uscita da un numero di abbonato che verrà bloccato da Parental Control :
     - **Chiamate e SMS**: blocca le chiamate e i messaggi SMS in uscita.
     - **Solo chiamate**: blocca solo le chiamate in uscita.
     - **Solo SMS**: blocca solo i messaggi SMS in uscita.

- **Numero di telefono**: numero di telefono che verrà bloccato per i messaggi SMS e/o le chiamate in uscita. Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

6. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA BLOCCATI

In caso di aggiunta accidentale di un numero alla Lista bloccati è possibile eliminare tale numero dalla lista. È possibile inoltre svuotare la Lista bloccati di Parental Control rimuovendo da essa tutte le voci.

Per eliminare una voce dalla Lista bloccati di Parental Control , eseguire le seguenti operazioni:

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.
4. Selezionare dalla lista la voce da eliminare e selezionare **Menu** → **Elimina**.
5. Confermare l'eliminazione premendo il pulsante **OK**.

Per svuotare la Lista bloccati:

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista bloccati**.

   Verrà aperta la finestra **Lista bloccati**.
4. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

CREAZIONE DI UNA LISTA CONSENTITI

È possibile creare una Lista consentiti in base alla quale Anti-Spam consente le chiamate e i messaggi SMS in entrata.

La lista contiene i numeri di telefono dei mittenti e le frasi che non si considerano come spam.

IN QUESTA SEZIONE

Aggiunta di voci alla Lista consentiti 157

Modifica di voci nella Lista consentiti 158

Eliminazione di voci dalla Lista consentiti 159

AGGIUNTA DI VOCI ALLA LISTA CONSENTITI

Tenere presente che lo stesso numero non può essere inserito contemporaneamente in entrambe la Lista bloccati e la Lista consentiti dei numeri di Parental Control . Se un numero è già stato salvato in una delle liste, Kaspersky Mobile Security 9.0 avvertirà l'utente – sullo schermo appariranno le relative informazioni.

Per aggiungere una voce alla Lista consentiti di Parental Control :

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare **Menu** → **Aggiungi** (vedere la figura sotto).

Figura 97. Aggiunta di voci alla Lista consentiti

Verrà aperta la finestra **Aggiungi voce**.

6. Selezionare i valori per le seguenti impostazioni (vedere la figura sotto).
   - **Consenti in uscita**: tipo di informazione in uscita che Parental Control consente di inviare a un numero di abbonato:
     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in uscita.
     - **Solo chiamate**: consente solo le chiamate in uscita.
     - **Solo SMS**: consente solo i messaggi SMS in uscita.

- **Numero di telefono**: numero di telefono al quale i messaggi SMS e/o le chiamate in uscita sono consentite da Parental Control . Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

Figura 98. Impostazioni della voce

7. Premere **OK** per salvare le modifiche.

MODIFICA DI VOCI NELLA LISTA CONSENTITI

È possibile cambiare i valori di tutte le impostazioni relative ai numeri presenti nella Lista consentiti.

Per modificare una voce della Lista consentiti di Parental Control :

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare dalla lista la voce che si desidera modificare e selezionare **Menu** → **Modifica**.

   Verrà aperta la finestra **Modifica voce**.
6. Modificare le impostazioni necessarie:
   - **Consenti in uscita**: tipo di informazione in uscita che Parental Control consente di inviare a un numero di abbonato:
     - **Chiamate e SMS**: consente le chiamate e i messaggi SMS in uscita.
     - **Solo chiamate**: consente solo le chiamate in uscita.
     - **Solo SMS**: consente solo i messaggi SMS in uscita.

- **Numero di telefono**: numero di telefono al quale i messaggi SMS e/o le chiamate in uscita sono consentite da Parental Control . Il numero di telefono deve comprendere solo caratteri alfanumerici; può iniziare con una cifra, una lettera o essere preceduto dal simbolo "+". In caso di numero, è possibile anche usare i caratteri jolly "*" o "?" (dove "*" rappresenta un numero qualsiasi di simboli e "?" qualsiasi singolo simbolo).

7. Premere **OK** per salvare le modifiche.

ELIMINAZIONE DI VOCI DALLA LISTA CONSENTITI

È possibile rimuovere una voce o svuotare completamente la Lista consentiti.

Per eliminare una voce dalla Lista consentiti di Parental Control :

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare dalla lista la voce da eliminare e selezionare **Menu** → **Elimina**.
6. Confermare l'eliminazione premendo il pulsante **OK**.

Per svuotare la Lista consentiti:

1. Selezionare **Menu** → **Parental Control**.
2. Verrà aperta la finestra **Parental Control**.
3. Selezionare l'opzione **Lista consentiti**.
4. Verrà aperta la finestra **Lista consentiti**.
5. Selezionare **Menu** → **Elimina tutto**.

La lista verrà svuotata.

PROTEZIONE DEI DATI IN CASO DI SMARRIMENTO O FURTO DEL DISPOSITIVO

Questa sezione fornisce informazioni sul componente Antifurto che assicura una protezione complessa dei dati personali in caso di furto o smarrimento del dispositivo e facilita la ricerca del dispositivo stesso. La sezione spiega inoltre come abilitare/disabilitare la funzione Antifurto, come impostare i parametri di funzionamento e come avviare la protezione da remoto in caso di furto o smarrimento del dispositivo.

IN QUESTA SEZIONE

Informazioni su Antifurto 160

Blocco del dispositivo 161

Eliminazione dei dati personali 162

Creazione di un elenco di dati eliminati 165

Monitoraggio della sostituzione di una scheda SIM sul dispositivo 166

Determinazione delle coordinate geografiche del dispositivo 167

Avvio remoto delle funzioni di Antifurto 169

INFORMAZIONI SU ANTIFURTO

Il componente Antifurto protegge i dati memorizzati nel dispositivo da accessi non autorizzati. Questa funzione può essere utile in caso di smarrimento o furto del dispositivo. Antifurto consente il blocco da remoto del dispositivo e la cancellazione dei dati memorizzati su di esso.

Questo componente comprende le seguenti funzioni:

- **SMS-Block**: consente di bloccare il dispositivo su richiesta dell'utente e di specificare un testo da visualizzare sullo schermo in modalità blocco.
- **SMS-Clean**: consente di cancellare in modo irreversibile dal dispositivo i dati personali dell'utente (tutti i contatti, messaggi, galleria, calendario, registri e impostazioni di accesso alla rete), i dati contenuti nelle schede di memoria e i file presenti nelle cartelle selezionate.
- **SIM Watch**: avvisa l'utente e blocca il dispositivo derubato se viene sostituita la scheda SIM o se il dispositivo viene acceso senza la scheda SIM. La funzione SIM Watch invia un messaggio contenente il nuovo numero di telefono del dispositivo a un numero di telefono specificato e/o a un indirizzo e-mail.
- **SMS-Find**: consente all'utente di determinare in remoto la posizione del dispositivo, che può essere inviata tramite messaggio al dispositivo richiedente o a un indirizzo e-mail specificato.

  Questa opzione funziona solo su dispositivi con ricevitore GPS integrato.

Per poter utilizzare tutte le funzioni di Antifurto, è necessario ricordare la password segreta creata alla prima esecuzione di Kaspersky Mobile Security 9.0.

Dopo l'installazione di Kaspersky Mobile Security 9.0, tutte le funzioni di Antifurto sono disabilitate.

Inoltre, Kaspersky Mobile Security 9.0 consente di avviare in remoto la funzione Antifurto inviando un comando al dispositivo smarrito o derubato (vedere la sezione "Avvio remoto delle funzioni Antifurto" a pagina 169).

Lo stato corrente di ogni funzione viene visualizzato nella finestra **Antifurto** accanto al nome della funzione.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

BLOCCO DEL DISPOSITIVO

In caso di smarrimento o furto del dispositivo, la funzione SMS-Block consente il blocco da remoto dell'accesso al dispositivo e ai dati memorizzati su di esso. Il dispositivo può essere sbloccato solo dopo aver immesso la password segreta.

Questa funzione non blocca il dispositivo ma abilita semplicemente l'opzione di blocco da remoto.

Per abilitare la funzione SMS-Block :

1. Selezionare **Menu** → **Antifurto**.

   Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Block**.

   Verrà aperta la finestra **SMS-Block**.

3. Selezionare la casella **Abilita SMS-Block**.

4. Immettere il messaggio da visualizzare sullo schermo del dispositivo in modalità blocco nel campo **Testo quando bloccato** (vedere la figura sotto). Per impostazione predefinita, per il messaggio verrà utilizzato il testo standard in cui è possibile aggiungere il numero di telefono del proprietario.

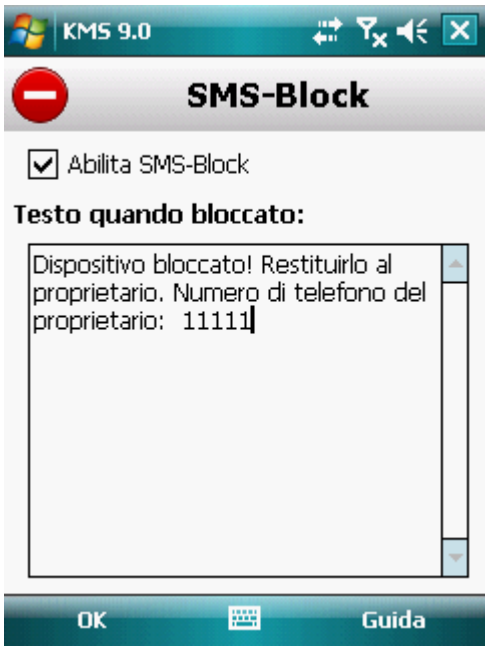


Figura 99. Impostazioni della funzione SMS-Block

5. Premere **OK** per salvare le modifiche.

Se la funzione SMS-Block è abilitata, è possibile bloccare il dispositivo utilizzando i seguenti metodi:

- Utilizzando il comando Invia. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo da bloccare. La ricezione del messaggio SMS speciale sul dispositivo bloccato è invisibile all'utente.

- Utilizzando un telefono per inviare un messaggio SMS standard. Per eseguire questa operazione, è necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo da bloccare.

Per il blocco da remoto del dispositivo, si consiglia di utilizzare un metodo sicuro con l'aiuto del comando Invia che trasmette il comando e la password segreta in forma criptata .

- *Per inviare un comando al dispositivo smarrito o derubato:*

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Invia comando**.

   Verrà aperta la finestra **Invia comando**.

3. Selezionare per l'impostazione **Opzioni** il valore **Blocca** (vedere la figura sotto).

4. Nel campo **Numero di telefono**, immettere il numero di telefono del dispositivo che si desidera bloccare.

5. Nel campo **Password remota**, immettere la password segreta impostata sul dispositivo che riceverà il messaggio.

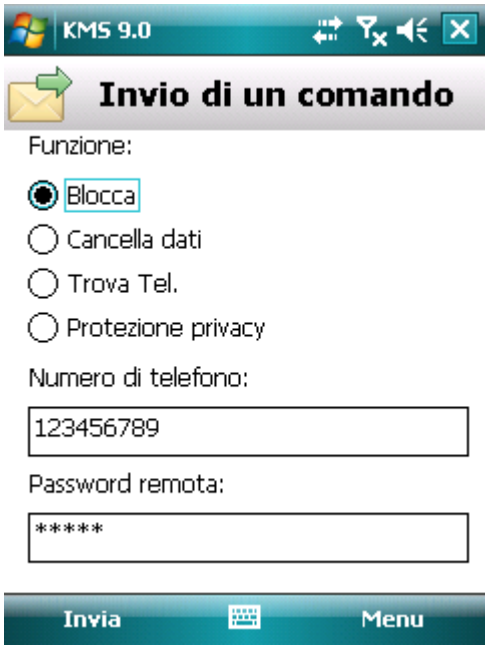


Figura 100. Avvio remoto di SMS-Block

6. Premere **Invia**.

- *Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,*

  inviare un messaggio SMS standard al dispositivo che si desidera bloccare. Il messaggio SMS deve contenere il testo `block:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

ELIMINAZIONE DEI DATI PERSONALI

In caso di furto o smarrimento del dispositivo mobile, la funzione SMS-Clean consente la cancellazione remota delle seguenti informazioni memorizzate sul dispositivo:

- dati personali dell'utente (tutti i contatti, messaggi, galleria, calendario e impostazioni di connessione alla rete), mentre Antifurto elimina i contatti memorizzati nella rubrica e sulla scheda SIM;

- dati contenuti nelle schede di memoria;
- file presenti nella cartella Documenti e in altre cartelle specificate.

Questa funzione non elimina i dati memorizzati sul dispositivo, ma include l'opzione di cancellazione.

Antifurto eliminerà i dati dall'elenco di oggetti da eliminare creato solo dopo che il dispositivo ha ricevuto il messaggio SMS speciale (vedere la sezione "Creazione di un elenco di oggetti da eliminare" a pagina 165).

Per abilitare la funzione SMS-Clean:

1. Selezionare **Menu** → **Antifurto**.

   Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Clean**.

   Verrà aperta la finestra **SMS-Clean**.

3. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **SMS-Clean**.

4. Selezionare la casella **Abilita SMS-Clean**.

5. Selezionare il tipo di dati da eliminare selezionando le caselle accanto alle impostazioni desiderate nella sezione **Elimina** (vedere la figura sotto):

   - per cancellare i dati personali, selezionare la casella **Dati personali**;
   - per cancellare i file presenti nella cartella Documenti e in altre cartelle specificate, selezionare la casella **Cartelle**.

Figura 101. Selezione del tipo di dati da eliminare

6. Premere **OK** per salvare le modifiche.

7. Passare alla creazione di un elenco di cartelle da eliminare (vedere la sezione "Creazione di un elenco di oggetti da eliminare" a pagina 165).

Abilitando la funzione, è possibile eliminare dal dispositivo i dati personali utilizzando i seguenti metodi:

- Utilizzando il comando Invia. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo. La ricezione del messaggio SMS speciale sul dispositivo derubato o smarrito è invisibile all'utente.

- Utilizzando un telefono per inviare un messaggio SMS standard. È necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo smarrito o derubato.

Per l'eliminazione remota dei dati personali, si consiglia di utilizzare un metodo sicuro con l'aiuto del comando Invia che trasmette il comando e la password segreta in forma criptata .

Per inviare un comando al dispositivo smarrito o derubato:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Invia comando**.

   Verrà aperta la finestra **Invia comando**.

3. Selezionare per l'impostazione **Opzioni** il valore SMS-Clean (vedere la figura sotto).

4. Nel campo **Numero di telefono**, immettere il numero di telefono del dispositivo su cui devono essere eliminati i dati.

5. Nel campo **Password remota**, immettere la password segreta impostata sul dispositivo che riceverà il messaggio.

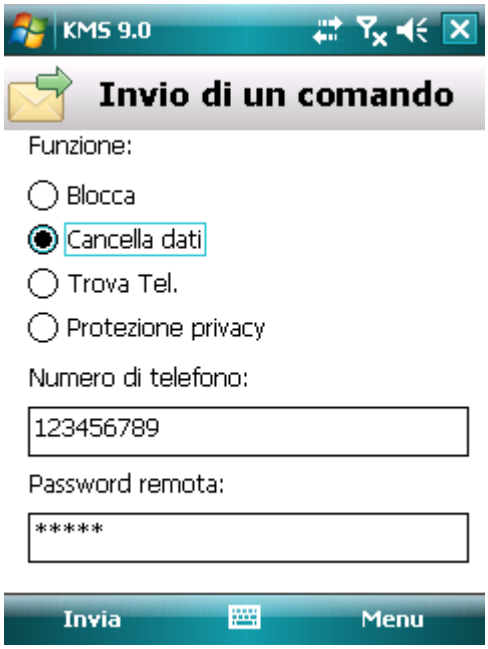


Figura 102. Avvio remoto di SMS-Clean

6. Premere **Invia**.

Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

inviare un messaggio SMS al dispositivo smarrito o derubato. Il messaggio SMS deve contenere il testo `wipe:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

CREAZIONE DI UN ELENCO DI DATI ELIMINATI

La funzione SMS-Clean consente di creare un elenco di cartelle da eliminare dopo la ricezione dello speciale messaggio SMS.

Per aggiungere una cartella all'elenco di cartelle da eliminare:

1. Selezionare **Menu** → **Antifurto**.

   Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Clean**.

   Verrà aperta la finestra **SMS-Clean**.

3. Selezionare l'opzione **Cartelle da eliminare**.

   Verrà aperta la finestra **Cartelle da eliminare**.

4. Selezionare **Menu** → **Aggiungi cartella** (vedere la figura sotto).

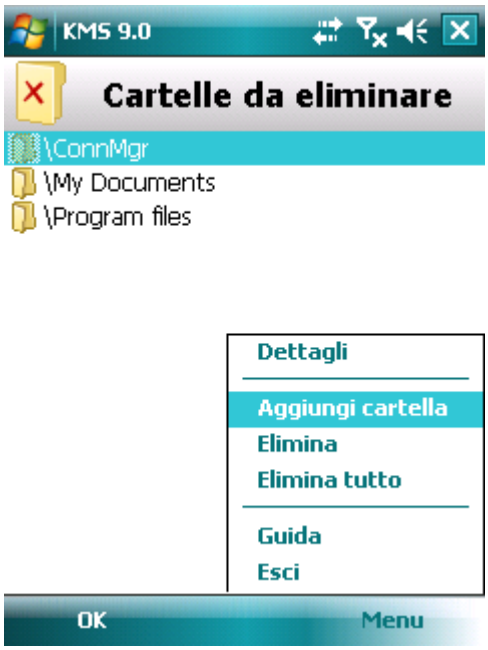


Figura 103. Selezione delle cartelle da eliminare

5. Selezionare la cartella desiderata dalla struttura di cartelle e premere**Seleziona**.

La cartella verrà aggiunta all'elenco.

Per rimuovere una cartella dall'elenco (vedere la figura sotto):

1. Selezionare **Menu** → **Antifurto**.

   Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Clean**.

   Verrà aperta la finestra **SMS-Clean**.

3. Selezionare l'opzione **Cartelle da eliminare**.

   Verrà aperta la finestra **Cartelle da eliminare**.

4. Selezionare una cartella dall'elenco e premere **Menu** → **Elimina**.

MONITORAGGIO DELLA SOSTITUZIONE DI UNA SCHEDA SIM SUL DISPOSITIVO

La funzione SIM Watch invia un messaggio contenente il nuovo numero della scheda SIM inserita a un numero di telefono e/o all'indirizzo e-mail specificato e blocca il dispositivo in caso di sostituzione della scheda SIM sul dispositivo smarrito o derubato.

Per abilitare la funzione SIM Watch e controllare la sostituzione della scheda SIM:

1. Selezionare **Menu** → **Antifurto**.

   Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SIM Watch**.

   Verrà aperta la finestra **SIM Watch**.

3. Selezionare la casella **Abilita SIM Watch**.

4. Per controllare la sostituzione della scheda SIM sul dispositivo, selezionare le seguenti impostazioni (vedere la figura sotto):

   - Per inviare automaticamente un messaggio sul nuovo numero di telefono, immettere il numero di telefono al quale deve essere inviato il messaggio nel campo **Numero di telefono** della sezione **Invia nuovo numero**.

     Il numero di telefono può iniziare con una cifra o con un "+" e deve contenere solo cifre.

   - Per ricevere un messaggio e-mail sul nuovo numero del proprio telefono, immettere un indirizzo e-mail nel campo **Indirizzo e-mail** della sezione **Invia nuovo numero**.

   - Per bloccare il dispositivo quando la scheda SIM viene sostituita o quando il dispositivo viene acceso senza una scheda, per l'impostazione **Durante sostituzione scheda SIM**, selezionare la casella **Blocca**. È possibile sbloccare il dispositivo solo dopo aver immesso la password segreta.

   - Per visualizzare un messaggio sullo schermo in modalità blocco, inserirlo nel campo **Testo quando bloccato**. Per impostazione predefinita, per il messaggio verrà utilizzato il testo standard in cui è possibile aggiungere il numero di telefono del proprietario.

Figura 104. Impostazioni della funzione SIM Watch

5. Premere **OK** per salvare le modifiche.

DETERMINAZIONE DELLE COORDINATE GEOGRAFICHE DEL DISPOSITIVO

La funzione SMS-Find è in grado di inviare le coordinate geografiche del dispositivo a un dispositivo richiedente mediante un messaggio SMS e/o a un indirizzo e-mail specificato.

Questa opzione funziona solo su dispositivi con ricevitore GPS integrato. Se necessario, il ricevitore sarà attivato automaticamente.

Le coordinate possono essere ottenute solo se il dispositivo si trova in un'area coperta da satelliti. Se non sono disponibili satelliti al momento della richiesta, verranno effettuati dei tentativi di ricerca ad intervalli specifici.

➧ *Per abilitare la funzione SMS-Find:*

1. Selezionare **Menu** → **Antifurto**.

   Verrà aperta la finestra **Antifurto**.

2. Selezionare l'opzione **SMS-Find**.

   Verrà aperta la finestra **SMS-Find**.

3. Selezionare la casella **Abilita SMS-Find**.

   Per impostazione predefinita, Kaspersky Mobile Security 9.0 invia le coordinate del dispositivo in risposta a un messaggio SMS.

4. Per ricevere le coordinate del dispositivo anche via e-mail, immettere l'indirizzo e-mail per l'impostazione **Invia coordinate** (vedere la figura sotto).

Figura 105. Impostazioni della funzione SMS-Find

5. Premere **OK** per salvare le modifiche.

È possibile richiedere le coordinate di un dispositivo su cui è abilitata la funzione SMS-Find utilizzando i seguenti metodi:

- Utilizzando il comando Invia. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo. La ricezione del messaggio SMS speciale sul dispositivo derubato o smarrito è invisibile all'utente.

- Opzioni standard di creazione dei messaggi SMS sul telefono. È necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo smarrito o derubato.

Per determinare in remoto le coordinate del dispositivo, si consiglia di utilizzare un metodo sicuro con l'aiuto del comando Invia che trasmette il comando e la password segreta in forma criptata .

Per inviare un comando al dispositivo smarrito o derubato:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Invia comando**.

   Verrà aperta la finestra **Invia comando**.

3. Selezionare per l'impostazione **Funzione** il valore **Trova Tel.** (vedere la figura sotto).

4. Nel campo **Numero di telefono**, immettere il numero di telefono del dispositivo di cui devono essere ricevute le coordinate.

5. Nel campo **Password remota**, immettere la password segreta impostata sul dispositivo che riceverà il messaggio.

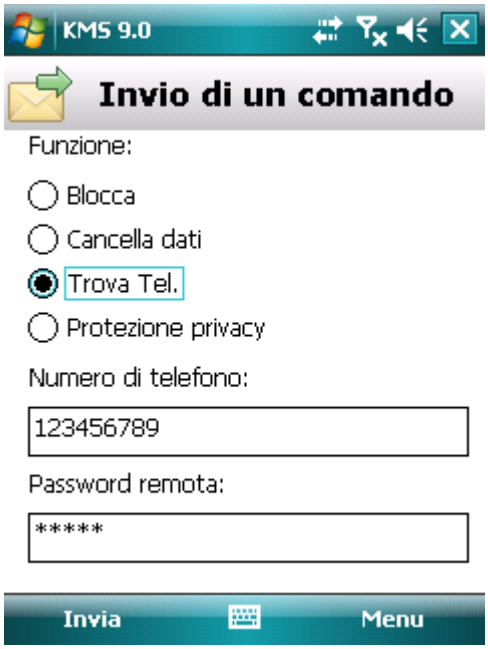


Figura 106. Determinazione della posizione del dispositivo

6. Premere **Invia**.

Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,

inviare un messaggio SMS al dispositivo smarrito o derubato. Il messaggio SMS deve contenere il testo `find:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo da bloccare. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

Verrà inviato un messaggio SMS con le coordinate del dispositivo al numero da cui è stata inviata la richiesta di ricevere le coordinate e all'indirizzo e-mail, se specificato nelle impostazioni SMS-Find.

AVVIO REMOTO DELLE FUNZIONI DI ANTIFURTO

È possibile inviare un comando con uno speciale messaggio SMS per avviare da remoto la funzione Antifurto sul dispositivo smarrito o derubato su cui è installato Kaspersky Mobile Security. Il comando viene ricevuto sul dispositivo bloccato in modo invisibile all'utente.

Si consiglia di utilizzare la funzione Invia comando in quanto il comando e la password segreta del dispositivo derubato o smarrito vengono trasmessi in forma criptata .

Per inviare un comando al dispositivo smarrito o derubato:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Invia comando**.

3. Verrà aperta la finestra **Invia comando**.

4. Selezionare uno dei valori suggeriti per l'impostazione **Funzione** (vedere la figura sotto):

- **SMS-Block** .
- **SMS-Clean** .
- **SMS-Find** (vedere la sezione "Determinazione delle coordinate geografiche del dispositivo" a pagina 167).
- **Protezione privacy** (vedere la sezione "Mascheramento dei dati personali" a pagina 170).

5. Nel campo **Numero di telefono**, immettere il numero di telefono del dispositivo al quale deve essere inviato il messaggio SMS.
6. Nel campo **Password remota**, immettere la password segreta impostata sul dispositivo che riceverà il messaggio.

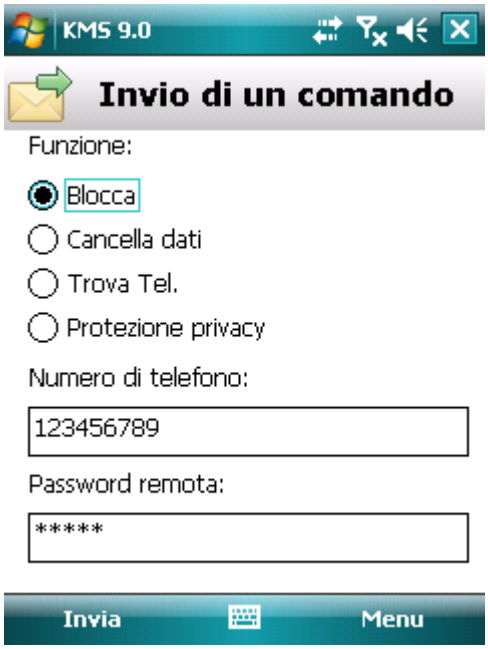


Figura 107. Avvio remoto delle funzioni di Antifurto

7. Premere **Invia**.

MASCHERAMENTO DEI DATI PERSONALI

Questa sezione fornisce informazioni su Protezione privacy. Il componente abilita il mascheramento dei dati riservati dell'utente mentre il dispositivo viene utilizzato temporaneamente da un'altra persona.

IN QUESTA SEZIONE

Protezione privacy 171

Modalità di Protezione privacy 171

Abilitazione/disabilitazione di Protezione privacy 172

Avvio automatico di Protezione privacy 173

Avvio remoto di Protezione privacy 174

Creazione di un elenco di contatti protetti 175

Selezione degli oggetti di protezione: Protezione privacy 178

PROTEZIONE PRIVACY

Il componente Protezione privacy protegge i dati personali dell'utente e impedisce l'accesso indesiderato alle informazioni personali mentre altre persone utilizzano temporaneamente il dispositivo. Il componente abilita il mascheramento dei dati riservati dell'utente, come i contatti (salvati nella memoria del dispositivo, sulla scheda SIM o su un supporto rimovibile), i messaggi e le chiamate.

Il componente analizza i dati personali in base all'elenco di numeri protetti (vedere la sezione "Creazione di un elenco di contatti protetti" a pagina 175). Il componente nasconde le seguenti informazioni relative ai numeri di questo elenco:

- informazioni nell'elenco contatti;
- voce del numero nel registro chiamate (in entrata, in uscita, perse).
- messaggi SMS nell'elenco dei messaggi SMS in entrata, in uscita, eliminati e inviati.

Le informazioni sul funzionamento di Protezione privacy vengono memorizzate nel report (vedere "Report dell'applicazione" a pagina 191).

MODALITÀ DI PROTEZIONE PRIVACY

Kaspersky Mobile Security 9.0 consente di gestire la protezione dei dati personali dell'utente. Il componente Protezione privacy viene avviato manualmente. Per impostazione predefinita, è disabilitato.

Protezione privacy può funzionare in una delle seguenti modalità:

- **Normale**: la protezione dei dati riservati è disabilitata. Le impostazioni di Protezione privacy sono accessibili per la modifica.
- **Privato**: la protezione dei dati riservati è abilitata. Il componente Protezione privacy nasconde tutti i dati relativi ai contatti protetti. Le impostazioni di Protezione privacy non possono essere modificate.

La modalità di funzionamento corrente del componente è visualizzata nella finestra **Protezione privacy** accanto alla voce del menu **Modo**.

La modifica della modalità di Protezione privacy può richiedere un certo tempo.

ABILITAZIONE/DISABILITAZIONE DI PROTEZIONE PRIVACY

La modalità di Protezione privacy può essere modificata come indicato di seguito:

- dal menu delle impostazioni del componente;
- dal menu **Protezione privacy**.

Per modificare la modalità di Protezione privacy:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **Modalità**.

3. Selezionare un valore per l'impostazione **Modalità** (vedere la figura sotto).

4. Premere **OK**.

Figura 108. Modifica della modalità di Protezione privacy

5. Confermare la modifica della modalità di Protezione privacy premendo il pulsante **OK**.

Per modificare rapidamente la modalità di Protezione privacy:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Premere **Privato** / **Normale**. Il nome del pulsante cambia in base allo stato corrente del componente Protezione privacy.

3. Confermare la modifica della modalità di Protezione privacy premendo il pulsante **OK**.

AVVIO AUTOMATICO DI PROTEZIONE PRIVACY

La protezione dei dati riservati viene avviata per impostazione predefinita immediatamente dopo l'abilitazione di Protezione privacy.

È possibile impostare un tempo allo scadere del quale il componente Protezione privacy verrà avviato automaticamente.

Disabilitare il componente Protezione privacy prima di modificare le sue impostazioni.

Per configurare l'avvio automatico di Protezione privacy alla scadenza di un tempo specificato:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Modalità**.

3. Verrà aperta la finestra **Modalità**.

4. Selezionare la casella **Blocca accesso** (vedere la figura sotto).

5. Selezionare un tempo allo scadere del quale il componente Protezione privacy verrà abilitato automaticamente. Per eseguire questa operazione, impostare uno dei valori suggeriti per l'impostazione **Timeout**:

   - **Nessun ritardo**.
   - **Dopo 1 minuto**.
   - **Dopo 5 minuti**.
   - **Dopo 15 minuti**.
   - **Dopo 1 ora**.

Figura 109. Avvio automatico di Protezione privacy

6. Premere **OK**.

AVVIO REMOTO DI PROTEZIONE PRIVACY

Kaspersky Mobile Security 9.0 consente di avviare da remoto Protezione privacy tramite uno speciale messaggio SMS. Per eseguire questa operazione, abilitare prima la funzione che consente l'avvio remoto di Protezione privacy.

Per consentire l'avvio remoto di Protezione privacy:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **Modalità**.

3. Selezionare la casella **Nascondi su SMS** (vedere la figura sotto).

Figura 110. Impostazioni di abilitazione remota di Protezione privacy

4. Premere **OK**.

Il componente Protezione privacy può essere avviato in remoto come indicato di seguito:

- Inviando un comando al dispositivo smarrito o derubato. Ciò richiede un secondo dispositivo su cui è installato Kaspersky Mobile Security 9.0. Sul secondo dispositivo è necessario creare e inviare da Kaspersky Mobile Security 9.0 uno speciale messaggio SMS consistente nel numero di telefono e password segreta del dispositivo. La ricezione del messaggio SMS speciale sul dispositivo derubato o smarrito è invisibile all'utente.

- Opzioni standard di creazione dei messaggi SMS sul telefono. È necessario creare e inviare sul secondo dispositivo un messaggio SMS contenente il testo speciale e la password segreta del dispositivo smarrito o derubato.

Per inviare un comando al dispositivo smarrito o derubato:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Invia comando**.

Verrà aperta la finestra **Invia comando**.

3. Selezionare per l'impostazione **Funzione** il valore **Protezione privacy** (vedere la figura sotto).

4. Nel campo **Numero di telefono**, immettere il numero di telefono del dispositivo di cui devono essere ricevute le coordinate.

5. Nel campo **Password remota**, immettere la password segreta impostata sul dispositivo che riceverà il messaggio.

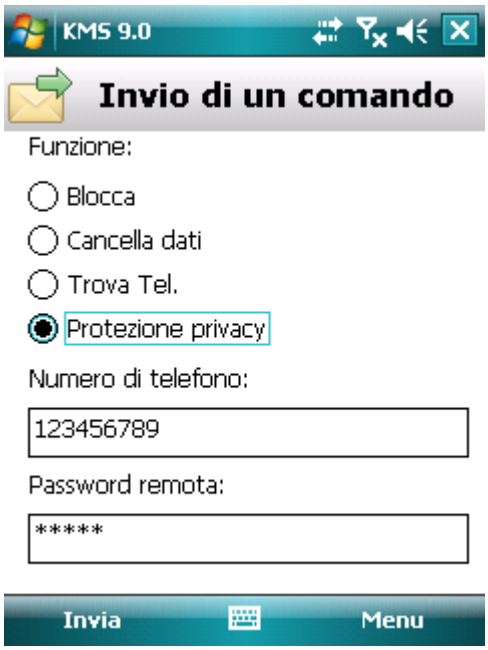


Figura 111. Avvio remoto di Protezione privacy

6. Premere **Invia**.

Alla ricezione del comando, il componente Protezione privacy viene avviato automaticamente sul dispositivo smarrito o derubato.

➡ *Per creare un messaggio SMS con le funzioni standard di creazione SMS del telefono,*

inviare un messaggio SMS standard al dispositivo che si desidera rintracciare. Il messaggio SMS deve contenere il testo `hide:<codice>`, dove `<codice>` è la password segreta impostata sul dispositivo ricevente. Il messaggio non distingue tra maiuscole/minuscole e gli spazi prima o dopo i due punti vengono ignorati.

CREAZIONE DI UN ELENCO DI CONTATTI PROTETTI

Il componente Protezione privacy nasconde i dati personali (ad esempio, i messaggi SMS e le chiamate) collegati a determinati abbonati. I numeri degli abbonati vengono salvati nell'elenco dei contatti protetti.

IN QUESTA SEZIONE

Aggiunta di un numero all'elenco dei contatti protetti 176

Modifica di un numero nell'elenco dei contatti protetti 176

Eliminazione di un numero dall'elenco dei contatti protetti 177

AGGIUNTA DI UN NUMERO ALL'ELENCO DEI CONTATTI PROTETTI

Disabilitare il componente Protezione privacy prima di modificare le sue impostazioni.

Per aggiungere un numero di telefono all'elenco dei contatti protetti:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Elenco contatti**.

   Verrà aperta la finestra **Elenco contatti**.

3. Eseguire una delle seguenti operazioni (vedere la figura sotto):

   - Per aggiungere un numero dalla rubrica, selezionare **Menu** → **Aggiungi** → **Contatto Outlook**. Nella finestra **Elenco contatti** visualizzata, specificare la voce desiderata e premere **Seleziona**.
   - Per aggiungere un numero salvato sulla scheda SIM, selezionare **Menu** → **Aggiungi** → **Contatto da SIM**. Nella finestra **Contatto da SIM** visualizzata, selezionare la voce desiderata e premere **OK**.
   - Per aggiungere un numero manualmente, selezionare **Menu** → **Aggiungi** → **Numero**. Nella finestra **Aggiungi voce** visualizzata, compilare il campo **Numero di telefono** e premere **OK**.

Figura 112. Aggiunta di voci all'elenco dei contatti protetti

Il numero di telefono verrà aggiunto all'elenco dei contatti protetti.

MODIFICA DI UN NUMERO NELL'ELENCO DEI CONTATTI PROTETTI

Disabilitare il componente Protezione privacy prima di modificare le sue impostazioni.

È possibile modificare solo i numeri di telefono immessi manualmente. Non è possibile modificare i numeri aggiunti dall'elenco contatti o da un elenco di numeri sulla scheda SIM.

Per modificare un numero di telefono nell'elenco dei contatti protetti:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Elenco contatti**.

   Verrà aperta la finestra **Elenco contatti**.

3. Selezionare il numero da modificare e selezionare **Menu** → **Modifica numero**.

   Verrà aperta la finestra **Modifica voce**.

4. Modificare i dati nel campo **Numero di telefono**.

5. Al termine della modifica, premere **OK**.

Il numero verrà modificato.

ELIMINAZIONE DI UN NUMERO DALL'ELENCO DEI CONTATTI PROTETTI

È possibile eliminare uno o tutti i numeri dall'elenco dei contatti protetti.

Disabilitare il componente Protezione privacy prima di modificare le sue impostazioni.

Per eliminare un numero di telefono dall'elenco dei contatti protetti:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Elenco contatti**.

3. Verrà aperta la finestra **Elenco contatti**.

4. Selezionare il numero da eliminare e selezionare **Menu** → **Rimuovi voce**.

5. Confermare l'eliminazione premendo il pulsante **OK**.

Per svuotare l'elenco dei contatti protetti:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Elenco contatti**.

3. Verrà aperta la finestra **Elenco contatti**.

4. Selezionare **Menu** → **Elimina tutto**.

5. Confermare l'eliminazione premendo il pulsante **OK**.

L'elenco dei contatti protetti verrà svuotato.

SELEZIONE DEGLI OGGETTI DI PROTEZIONE: PROTEZIONE PRIVACY

Quando il componente Protezione privacy è abilitato, i contatti, i messaggi e le voci nei registri chiamate relativi ai contatti protetti sono nascosti per impostazione predefinita. È possibile selezionare i dati il cui accesso è limitato.

Disabilitare il componente Protezione privacy prima di modificare le sue impostazioni.

Per selezionare gli oggetti di protezione:

1. Selezionare **Menu** → **Protezione privacy**.

   Verrà aperta la finestra **Protezione privacy**.

2. Selezionare l'opzione **Oggetti nascosti**.

   Verrà aperta la finestra **Oggetti nascosti** (vedere la figura sotto).

3. Nella sezione **Nascondi voci**, selezionare i dati memorizzati sul dispositivo che deve essere nascosto. Sono disponibili le seguenti opzioni:

   - **Contatti**: nasconde nella rubrica del dispositivo tutti i dati sui numeri protetti.
   - **SMS**: nasconde nell'elenco dei messaggi in entrata/uscita tutti i messaggi SMS dai numeri protetti.
   - **Chiamate**: accetta le chiamate dai numeri protetti, ma nasconde il numero del chiamante e non visualizza le informazioni sui numeri protetti nell'elenco delle chiamate (in entrata, in uscita, perse).

4. Nella sezione **Nascondi eventi**, selezionare i dati in entrata da nascondere. Sarà disponibile l'opzione per nascondere i seguenti eventi:

   - **SMS in entrata**: non visualizza il recapito dei messaggi SMS in entrata (sullo schermo non verrà visualizzato alcun messaggio sulla ricezione di un nuovo messaggio SMS da un numero nascosto). Tutti i messaggi SMS ricevuti dai numeri nascosti possono essere visualizzati se si disabilita la modalità Protezione privacy.

- **Chiamate in entrata**: blocca le chiamate dai numeri dell'Elenco contatti (in questo caso il chiamante udirà il segnale di occupato). Le informazioni sulle chiamate ricevute verranno visualizzate dopo aver disabilitato la protezione dei dati riservati.

Figura 113. Selezione di oggetti nascosti

5. Premere **OK**.

FILTRO DELL'ATTIVITÀ DI RETE. FIREWALL

Questa sezione fornisce informazioni sul componente Firewall che monitorizza le connessioni in entrata e in uscita sul dispositivo. La sezione spiega inoltre come abilitare/disabilitare il funzionamento del componente e come selezionare il livello di sicurezza richiesto.

IN QUESTA SEZIONE

Informazioni su Firewall 179

Abilitazione/disabilitazione di Firewall 180

Selezione del livello di sicurezza di Firewall 180

INFORMAZIONI SU FIREWALL

La funzione Firewall analizza tutte le connessioni di rete sul dispositivo bloccando o consentendo l'attività di rete in base al livello di sicurezza selezionato.

Al termine dell'installazione, il componente Firewall di Kaspersky Mobile Security 9.0 è disabilitato.

Le informazioni sul funzionamento di Firewall vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

ABILITAZIONE/DISABILITAZIONE DI FIREWALL

Il funzionamento di Firewall è basato su livelli di sicurezza. Il livello di sicurezza determina quali protocolli di rete possono essere utilizzati per trasferire le informazioni e quali di essi sono bloccati.

Sono disponibili i seguenti livelli di sicurezza:

- **Disabilitato**: tutte le attività di rete sono consentite. Questo è il livello di sicurezza predefinito selezionato.
- **Protezione min**.: vengono bloccate solo le connessioni in entrata. Le connessioni in uscita sono consentite.
- **Protezione max**: vengono bloccate tutte le connessioni in entrata. Sono accessibili il controllo delle e-mail, la visualizzazione di siti web e il download di file. Le connessioni in uscita possono essere stabilite solo mediate le porte SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Blocca tutto**: blocca tutte le attività di rete tranne l'aggiornamento del database dell'applicazione e il rinnovo della licenza.

È possibile cambiare il livello di sicurezza di Firewall (vedere la sezione "Selezione del livello di sicurezza di Firewall" a pagina 180). La modalità corrente è visualizzata nella finestra **Firewall** accanto alla voce del menu **Modalità**.

SELEZIONE DEL LIVELLO DI SICUREZZA DI FIREWALL

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per impostare il livello di sicurezza di Firewall:

1. Selezionare **Menu** → **Firewall**.

   Verrà aperta la finestra **Firewall**.

2. Selezionare l'opzione **Modalità**.

   Verrà aperta la finestra **Impostazioni**.

3. Selezionare uno dei livelli di sicurezza suggeriti (vedere la figura sotto).

Figura 114. Selezione del livello di sicurezza di Firewall

4. Premere **OK**.

CRIPTAGGIO DEI DATI PERSONALI

Questa sezione fornisce informazioni sul componente Criptaggio che protegge i dati riservati sul dispositivo. La sezione spiega inoltre come abilitare/disabilitare il funzionamento del componente e come criptare/decriptare le cartelle selezionate.

IN QUESTA SEZIONE

Informazioni sul componente Criptaggio 181

Criptaggio dei dati..... 182

Decriptaggio dei dati..... 183

Blocco dell'accesso ai dati criptati 184

INFORMAZIONI SUL COMPONENTE CRIPTAGGIO

Il componente Criptaggio protegge i dati sul dispositivo dalla visualizzazione da parte di altre persone che riescano ad avere accesso al dispositivo mobile. Il componente consente di criptare qualsiasi numero di cartelle non di sistema.

Per criptare/decriptare i dati, è necessario immettere la password segreta (vedere la sezione "Immissione della password segreta" a pagina 116). Dopo il passaggio del dispositivo alla modalità di risparmio energia, alla scadenza dell'ora impostata (vedere la sezione "Protezione dell'accesso ai dati criptati " a pagina 184), l'accesso ai dati viene automaticamente bloccato.

I dati nella cartella verranno criptati dopo l'esecuzione del comando **Cripta**. Successivamente, i dati verranno criptati e decriptati in tempo reale quando vengono spostati in una cartella, estratti da essa o al loro accesso.

Non è possibile eseguire i file eseguibili (.exe) da una cartella criptata .

Al termine dell'installazione, il componente Criptaggio di Kaspersky Mobile Security 9.0 è disabilitato.

Le informazioni sul funzionamento del componente vengono inserite nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

CRIPTAGGIO DEI DATI

Il componente Criptaggio consente di criptare qualsiasi numero di cartelle non di sistema presenti nella memoria del dispositivo o su una scheda di memoria.

L'elenco di tutti i file precedentemente criptati e decriptati è accessibile nella finestra **Criptaggio** da **Elenco cartelle**.

È possibile anche criptare immediatamente tutte le cartelle presenti nell'elenco delle cartelle.

Per criptare i dati:

1. Selezionare **Menu** → **Criptaggio**.

   Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Elenco cartelle**.

   Verrà aperta la finestra **Elenco cartelle**.

3. Premere **Menu** → **Aggiungi cartella**.

   Verrà aperta una schermata contenente la struttura dei file del sistema del dispositivo.

4. Selezionare la cartella da criptare e premere **Criptaggio** (vedere la figura sotto).

   Per spostarsi nel file system, utilizzare la penna a stilo o i pulsanti di spostamento del dispositivo.

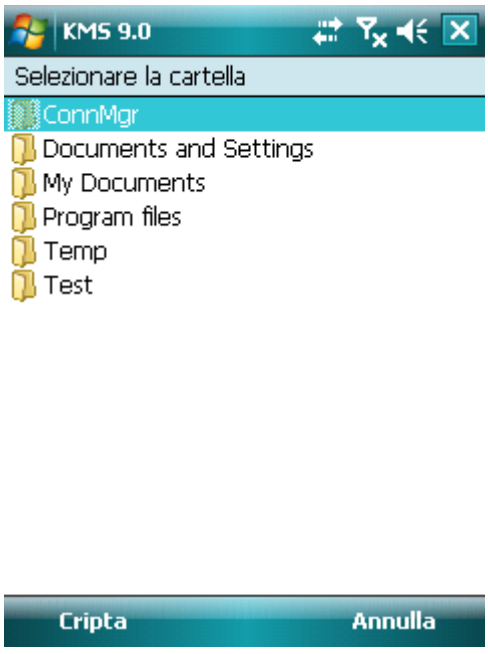


Figura 115. Criptaggio dei dati

Al termine della procedura di criptaggio , Kaspersky Mobile Security 9.0 informerà l'utente visualizzando una finestra di notifica.

5. Premere **OK**.

   Se la cartella è criptata , il nome dell'opzione **Cripta** cambia in **Decripta** nel **Menu**.

Dopo il processo di criptaggio , i dati verranno decriptati e criptati automaticamente alla loro apertura o spostamento dalla cartella criptata , oppure se si collocano nuovi dati nella cartella criptata .

- *Per criptare in un solo passaggio tutte le cartelle presenti nell'elenco, eseguire le seguenti operazioni:*

1. Selezionare **Menu** → **Criptaggio**.

   Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Elenco cartelle**.

   Verrà aperta la finestra **Elenco cartelle**.

3. Selezionare **Menu** → **Aggiungi azioni** → **Cripta tutto**.

   Al termine della procedura di criptaggio , Kaspersky Mobile Security 9.0 informerà l'utente visualizzando una finestra di notifica.

4. Premere **OK**.

DECRIPTAGGIO DEI DATI

È possibile decriptare completamente i dati criptati precedentemente (vedere la sezione "Criptaggio dei dati" a pagina 182). È possibile decriptare una o tutte le cartelle criptate presenti sul dispositivo.

- *Per decriptare una cartella precedentemente criptata :*

1. Selezionare **Menu** → **Criptaggio**.

   Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Elenco cartelle**.

   Verrà aperta la finestra **Elenco cartelle** contenente un elenco di tutte le cartelle precedentemente decriptate e criptate .

3. Selezionare una cartella decriptata dall'elenco e premere **Menu** → **Decripta** (vedere la figura sotto).

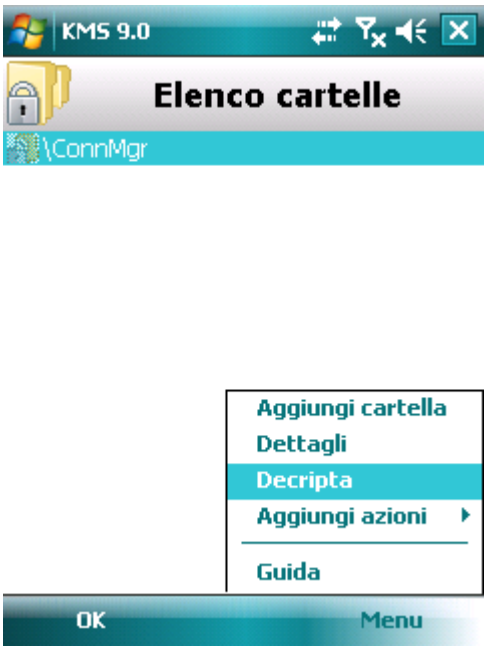


Figura 116. Abilitazione dell'opzione

Al termine della procedura di decriptaggio , Kaspersky Mobile Security 9.0 informerà l'utente visualizzando una finestra di notifica.

4. Premere **OK**.

Se la cartella è decriptata , il nome dell'opzione **Decripta** cambia in **Cripta** nel **Menu**. È possibile a questo punto criptare nuovamente i dati (vedere la sezione "Criptaggio dei dati" a pagina 182).

Per decriptare in un solo passaggio tutte le cartelle presenti nell'elenco, eseguire le seguenti operazioni:

1. Selezionare **Menu** → **Criptaggio** .

   Verrà aperta la finestra Criptaggio .

2. Selezionare l'opzione **Elenco cartelle**.

   Verrà aperta la finestra **Elenco cartelle**.

3. Selezionare **Menu** → **Aggiungi azioni** →Decripta **tutto**.

   Al termine della procedura di decriptaggio , Kaspersky Mobile Security 9.0 informerà l'utente visualizzando una finestra di notifica.

4. Premere **OK**.

BLOCCO DELL'ACCESSO AI DATI CRIPTATI

Il componente Criptaggio consente di bloccare l'accesso ai dati criptati immediatamente o alla scadenza dell'ora impostata dopo aver posto il dispositivo in modalità di risparmio energia.

Per impostazione predefinita, l'accesso ai dati criptati viene bloccato immediatamente dopo aver disabilitato la retroilluminazione.

È possibile impostare un'ora durante la quale i dati criptati rimangono accessibili dopo che il dispositivo è passato in modalità di risparmio energia. Per continuare ad utilizzare i dati criptati , è necessario immettere la password segreta (vedere la sezione "Immissione della password segreta" a pagina 116).

È possibile anche inibire momentaneamente l'accesso ai dati criptati e abilitare la richiesta della password segreta.

Per inibire l'accesso alla cartella con un ritardo temporale, eseguire le seguenti operazioni:

1. Selezionare **Menu** → **Criptaggio**.

   Verrà aperta la finestra **Criptaggio**.

2. Selezionare l'opzione **Blocca accesso**.

   Verrà aperta la finestra **Blocca accesso**.

3. Immettere il tempo dopo il quale il dispositivo entra in standby e in cui i dati sono accessibili. Per eseguire questa operazione, selezionare per l'impostazione **Blocca accesso** uno dei valori suggeriti (vedere la figura sotto):

   - **Nessun ritardo**.
   - **Dopo 1 minuto**.
   - **Dopo 5 minuti**.
   - **Dopo 15 minuti**.
   - **Dopo 1 ora**.

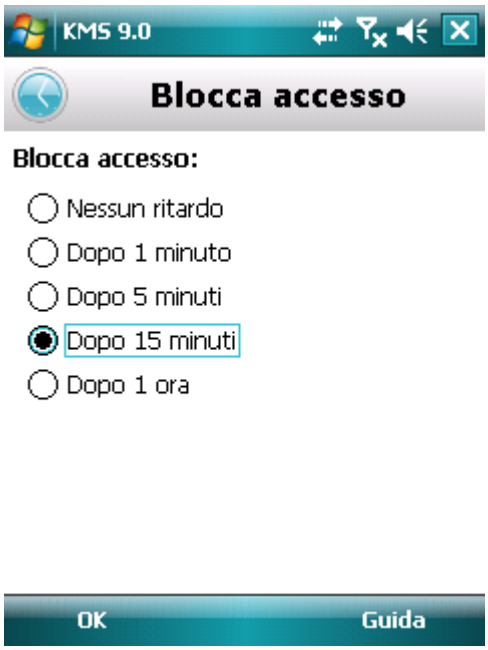


Figura 117. Blocco dell'accesso ai dati criptati

4. Premere **OK** per salvare le modifiche.

- *Per bloccare immediatamente l'accesso a una cartella,*

  premere l'icona di Kaspersky Mobile Security 9.0 nell'area di notifica del dispositivo e selezionare **Blocca dati** (vedere la figura sotto).

Figura 118. Menu di scelta rapida dell'applicazione nell'area di notifica del dispositivo

AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

Questa sezione fornisce informazioni sull'aggiornamento dei database dell'applicazione, che assicura la protezione aggiornata del dispositivo. La sezione specifica inoltre come visualizzare informazioni sui database dell'applicazione installati, come avviare manualmente il processo di aggiornamento e come configurare gli aggiornamenti automatici del database.

IN QUESTA SEZIONE

Informazioni sull'aggiornamento dei database dell'applicazione 186

Visualizzazione delle informazioni sul database 187

Aggiornamento manuale 188

Aggiornamento pianificato 189

Aggiornamento in roaming 190

INFORMAZIONI SULL'AGGIORNAMENTO DEI DATABASE DELL'APPLICAZIONE

L'applicazione esegue la scansione del dispositivo per individuare eventuali programmi malware utilizzando il database dell'applicazione, che contiene le descrizioni di tutti i programmi malware e di altri programmi indesiderati noti attualmente e i metodi per neutralizzarli. È quindi estremamente importante tenere aggiornato il database.

Si consiglia di aggiornare regolarmente i database dell'applicazione. Trascorsi più di 15 giorni dall'ultimo aggiornamento, i database verranno considerati come molto vecchi. Sarà quindi impossibile garantire una protezione affidabile.

Kaspersky Mobile Security 9.0 esegue l'aggiornamento dai server di aggiornamento di Kaspersky Lab. Si tratta di siti Internet dedicati contenenti gli aggiornamenti per i database di tutti i prodotti Kaspersky Lab.

Per aggiornare i database dell'applicazione è necessario disporre di una connessione Internet configurata sul proprio dispositivo mobile.

I database dell'applicazione vengono aggiornati mediante il seguente algoritmo:

1. I database dell'applicazione installati sul dispositivo mobile vengono confrontati a quelli situati sul server di aggiornamento dedicato di Kaspersky Lab.

2. Kaspersky Mobile Security 9.0 esegue una delle seguenti operazioni:

   - Se sono installati i database dell'applicazione più recenti, sullo schermo viene visualizzato un messaggio informativo.

   - Se i database installati sono diversi, viene scaricato e installato un nuovo pacchetto di aggiornamento.

     Al termine del processo di aggiornamento, la connessione viene automaticamente chiusa. Se la connessione è stata stabilita prima dell'avvio dell'aggiornamento, rimarrà aperta per ulteriore utilizzo.

È possibile avviare l'operazione di aggiornamento manualmente in qualsiasi momento mentre il dispositivo è occupato con altre operazioni oppure pianificare aggiornamenti automatici.

Informazioni dettagliate sui database sono disponibili nella finestra **Avanzate** dall'opzione **Info database**.

Le informazioni sugli aggiornamenti dei database vengono registrate nel report dell'applicazione (vedere la sezione "Report dell'applicazione" a pagina 191).

VISUALIZZAZIONE DELLE INFORMAZIONI SUL DATABASE

È possibile visualizzare informazioni sui database dell'applicazione installati. Sono disponibili le seguenti informazioni: data dell'ultimo aggiornamento, data di rilascio dei database e numero di voci nei database.

Per visualizzare le informazioni sui database installati:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare la scheda **Info database**.

Verrà aperta la finestra **Info database** con informazioni sui database del programma (vedere la figura sotto).

Figura 119. Informazioni sui database dell'applicazione installati

AGGIORNAMENTO MANUALE

È possibile avviare manualmente l'aggiornamento dei database dell'applicazione.

Per avviare il processo di aggiornamento del database:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Aggiornamento**.

   Verrà aperta la finestra **Aggiornamento**.

3. Selezionare l'opzione **Aggiornamento** (vedere la figura sotto).

Figura 120. Avvio manuale dell'aggiornamento

L'applicazione avvia il processo di aggiornamento dei database dal server Kaspersky Lab. Le informazioni sul processo di aggiornamento vengono visualizzate sullo schermo.

AGGIORNAMENTO PIANIFICATO

L'esecuzione regolare degli aggiornamenti è il requisito di base per l'efficace protezione del dispositivo contro le infezioni di oggetti malware. Per maggiore comodità, è possibile configurare aggiornamenti automatici del database.

➧ *Per configurare una pianificazione per gli aggiornamenti automatici del database:*

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Aggiornamento**.

   Verrà aperta la finestra **Aggiornamento**.

3. Selezionare l'opzione **Pianifica aggiornamento**.

   Verrà aperta la finestra **Pianifica**.

4. Selezionare la casella **Aggiornamento pianificato** (vedere la figura sotto).

5. Creare una pianificazione per l'esecuzione degli aggiornamenti selezionando un valore per l'impostazione **Frequenza**:

   - **Giornaliero**: aggiorna il database dell'applicazione ogni giorno. Immettere quindi un valore per l'impostazione **Ora**.

   - **Settimanale**: esegue l'aggiornamento una volta alla settimana. Selezionare quindi un valore per le impostazioni **Ora** e **Giorno della settimana**.

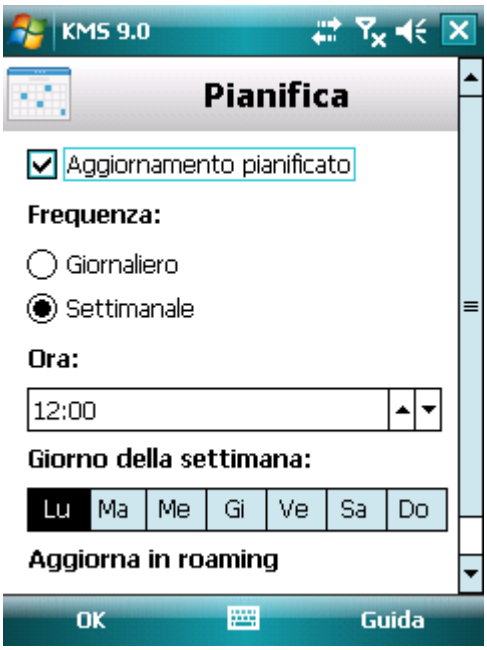


Figura 121. Impostazioni di aggiornamento automatico

6. Premere **OK** per salvare le modifiche.

AGGIORNAMENTO IN ROAMING

Quando il dispositivo si trova in una zona roaming, è possibile disabilitare gli aggiornamenti pianificati del database dell'applicazione. Se l'aggiornamento in roaming è bloccato, l'aggiornamento manuale è accessibile in modalità standard.

Per disabilitare gli aggiornamenti pianificati quando il dispositivo si trova in una zona roaming, eseguire le seguenti operazioni:

1. Selezionare **Menu** → **Anti-Virus**.

   Verrà aperta la finestra **Anti-Virus**.

2. Selezionare l'opzione **Aggiornamento**.

   Verrà aperta la finestra **Aggiornamento**.

3. Selezionare l'opzione **Pianifica aggiornamento**.

   Verrà aperta la finestra **Pianifica**.

4. Nella sezione **Aggiorna in roaming**, selezionare la casella **Aggiorna in roaming**.

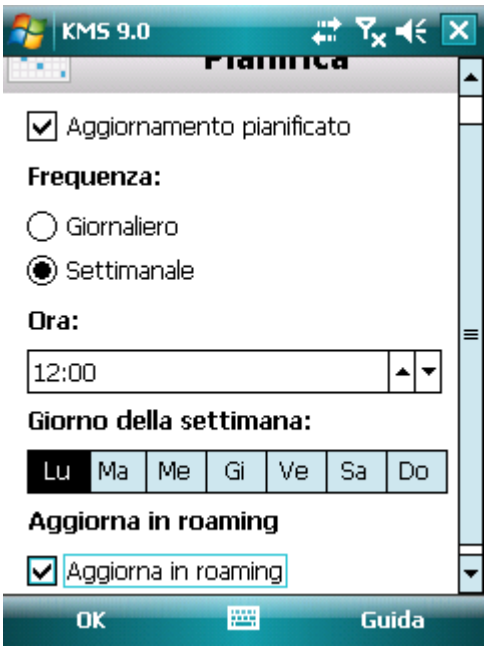


Figura 122. Configurazione degli aggiornamenti in roaming

5. Premere **OK** per salvare le modifiche.

REPORT DELL'APPLICAZIONE

Questa sezione fornisce informazioni sui report in cui viene registrato il funzionamento di ogni componente e l'esecuzione di ogni attività (ad esempio, gli aggiornamenti del database dell'applicazione, le scansioni anti-virus, ecc.).

IN QUESTA SEZIONE

Informazioni sui report 191

Visualizzazione dei record del report 191

Eliminazione dei record del report 192

INFORMAZIONI SUI REPORT

Nei report dell'applicazione vengono memorizzati i record relativi agli eventi che si verificano durante il funzionamento di Kaspersky Mobile Security. Le voci vengono ordinate in base all'ora dell'evento e a partire dagli eventi più recenti.

Per ogni componente viene utilizzato un report eventi distinto.

VISUALIZZAZIONE DEI RECORD DEL REPORT

➧ *Per visualizzare tutti i record memorizzati nel report:*

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Report**.

Verrà aperta la finestra **Report**.

3. Selezionare il componente del quale si desidera visualizzare il report eventi.

Verrà aperto il report eventi del componente selezionato (vedere la figura sotto).

Figura 123. Visualizzazione dei record nei report

- *Per visualizzare informazioni dettagliate sui record del report,*

  selezionare il record desiderato e premere **Dettagli**.

- *Per tornare ai report,*

  premere **Menu** → **Indietro**.

ELIMINAZIONE DEI RECORD DEL REPORT

È possibile svuotare tutti i report. Le informazioni sul funzionamento di tutti i componenti di Kaspersky Mobile Security 9.0 verranno eliminate.

- *Per cancellare tutti i report:*

  1. Selezionare **Menu** → **Avanzate**.

     Verrà aperta la finestra **Avanzate**.

  2. Selezionare l'opzione **Report**.

     Verrà aperta la finestra **Report**.

  3. Aprire il report di un qualunque componente.

4. Selezionare **Menu→ Elimina tutto** (vedere la figura sotto).

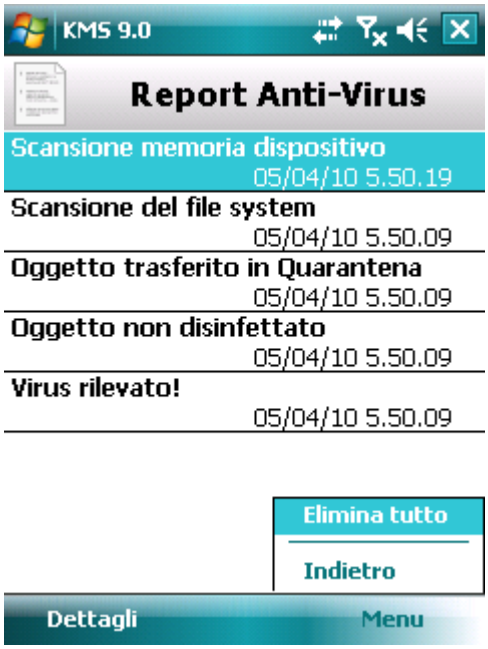


Figura 124. Eliminazione dei record

5. Confermare la cancellazione premendo il pulsante **Sì**.

Verranno eliminati tutti i record in tutti i report dei componenti.

CONFIGURAZIONE DI IMPOSTAZIONI AGGIUNTIVE

Questa sezione fornisce informazioni sulle opzioni aggiuntive di Kaspersky Mobile Security 9.0: come gestire le notifiche acustiche dell'applicazione e come abilitare/disabilitare la visualizzazione dei suggerimenti.

IN QUESTA SEZIONE

Modifica della password segreta 193

Visualizzazione dei suggerimenti 194

Configurazione delle notifiche acustiche 195

MODIFICA DELLA PASSWORD SEGRETA

È possibile modificare la password segreta impostata dopo l'attivazione dell'applicazione.

➧ *Per modificare la password segreta:*

1. Selezionare **Menu → Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Impostazioni**.

   Verrà aperta la finestra **Impostazioni**.

3. Selezionare l'opzione **Cambia password**.

4. Immettere il codice corrente nel campo di immissione **Immetti password**.

5. Immettere la nuova password nei campi **Immettere nuova password** e **Conferma password**, quindi premere **OK** per salvare le modifiche.

VISUALIZZAZIONE DEI SUGGERIMENTI

Quando si configurano le impostazioni dei componenti, Kaspersky Mobile Security 9.0 visualizza un messaggio predefinito con una descrizione sintetica della funzione selezionata. È possibile configurare la visualizzazione dei suggerimenti di Kaspersky Mobile Security 9.0.

Per configurare la visualizzazione dei suggerimenti, eseguire le seguenti operazioni:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Impostazioni**.

   Verrà aperta la finestra **Impostazioni**.

3. Selezionare l'opzione **Suggerimenti**.

   Verrà aperta la finestra **Suggerimenti**.

4. Selezionare uno dei valori suggeriti per l'impostazione **Suggerimenti**:

   - **Mostra**: visualizza i suggerimenti prima di configurare le impostazioni della funzione selezionata.
   - **Nascondi**: non visualizza i suggerimenti.

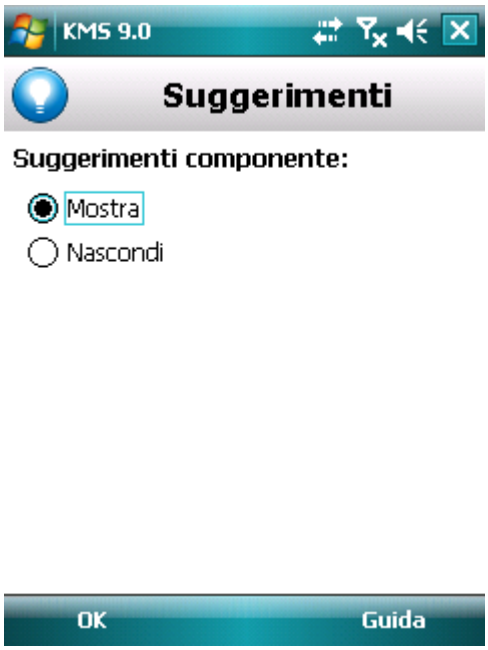


Figura 125. Impostazioni di visualizzazione dei suggerimenti

5. Premere **OK**.

CONFIGURAZIONE DELLE NOTIFICHE ACUSTICHE

In seguito al funzionamento dell'applicazione, si verificano eventi specifici: ad esempio, è stato rilevato un oggetto infetto o un virus, il periodo di validità della licenza sta per scadere, ecc. Per specificare all'applicazione di informare l'utente di ogni evento del genere, è possibile abilitare l'emissione di notifiche acustiche al verificarsi degli eventi.

Per impostazione predefinita, Kaspersky Mobile Security 9.0 emette le notifiche acustiche solo in base alla modalità impostata sul dispositivo.

Per modificare i valori delle impostazioni, utilizzare i pulsanti di spostamento o la penna stilo del dispositivo.

Per gestire l'emissione di notifiche acustiche dell'applicazione, eseguire le seguenti operazioni:

1. Selezionare **Menu** → **Avanzate**.

   Verrà aperta la finestra **Avanzate**.

2. Selezionare l'opzione **Impostazioni**.

   Verrà aperta la finestra **Impostazioni**.

3. Selezionare l'opzione **Segnale acustico**.

4. Verrà aperta la finestra **Segnale acustico**.

5. Selezionare uno dei valori suggeriti per l'impostazione **Notifiche acustiche** (vedere la figura sotto):

   - **Abilita**: emette notifiche acustiche indipendentemente dal profilo del dispositivo selezionato.
   - **Disabilita**: non emette notifiche acustiche.

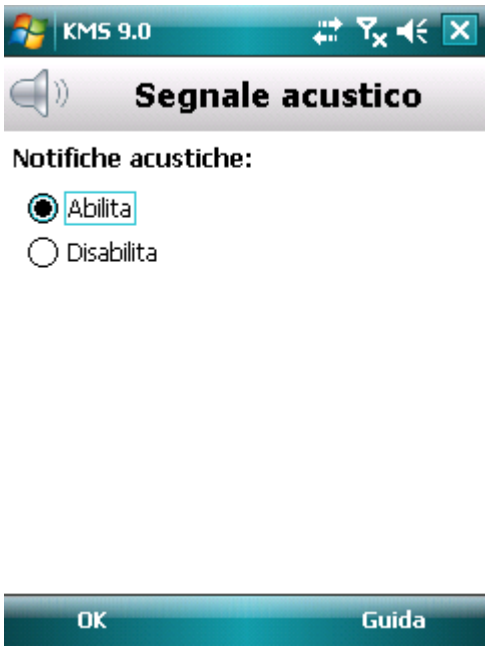


Figura 126. Gestione delle notifiche acustiche

6. Premere **OK** per salvare le modifiche.

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

Dopo l'acquisto di Kaspersky Internet Security, è possibile ottenere informazioni sull'applicazione tramite il Servizio di assistenza tecnica per telefono o via Internet.

Gli esperti del Servizio di assistenza tecnica risponderanno a tutte le domande relative all'installazione e all'utilizzo dell'applicazione. Gli esperti sono disponibili ad assistere l'utente nel processo di eliminazione delle conseguenze nocive delle attività del malware, nel caso in cui il dispositivo sia stato infettato.

Prima di contattare il Servizio di assistenza tecnica, leggere le regole sull'assistenza per i prodotti Kaspersky Lab (http://support.kaspersky.com/it/support/rules).

Invio di domande al Servizio di assistenza tecnica via e-mail

È possibile inoltrare le proprie domande agli esperti del Servizio di assistenza tecnica compilando l'apposito modulo dell'Helpdesk disponibile all'indirizzo (http://support.kaspersky.com/helpdesk.html?LANG=it).

È possibile scrivere le proprie domande in russo, inglese, tedesco, francese o spagnolo.

Per poter inviare un messaggio e-mail contenente la domanda, è necessario includere l'**ID cliente** e la **password** ricevuti al momento della registrazione sul sito Web del Servizio di assistenza tecnica.

Se non si è ancora utenti registrati delle applicazioni Kaspersky Lab, è possibile compilare un modulo di registrazione (https://support.kaspersky.com/en/personalcabinet/Registration/Form/?LANG=it). Durante la registrazione, immettere il *codice di attivazione* dell'applicazione o il *file chiave*.

Il Servizio di assistenza tecnica risponderà alle richieste nell'area Assistenza personalizzata (https://support.kaspersky.com/en/personalcabinet?LANG=it) e all'indirizzo e-mail specificato dall'utente nella propria richiesta.

Nella richiesta, descrivere il problema riscontrato. Specificare quanto segue nei campi obbligatori:

- **Tipo di richiesta**. Selezionare l'argomento corrispondente più da vicino al problema riscontrato, ad esempio "Problema di installazione/disinstallazione prodotto" o "Problema di scansione anti-virus/rimozione virus". Se non è disponibile un argomento appropriato, selezionare "Domanda generale".
- **Nome dell'applicazione e numero della versione**.
- **Testo della richiesta**. Descrivere il problema riscontrato fornendo quanti più dettagli possibile.
- **ID cliente e password**. Immettere l'ID cliente e la password ricevuti al momento della registrazione sul sito Web del Servizio di assistenza tecnica.
- **Indirizzo e-mail**. Il Servizio di assistenza tecnica risponderà alla domanda a questo indirizzo e-mail.

Assistenza tecnica per telefono

Per problemi urgenti, è possibile contattare il Servizio di assistenza tecnica locale. Prima di contattare il Servizio di assistenza tecnica locale (http://support.kaspersky.com/support/support_local) o internazionale (http://support.kaspersky.com/support/international), raccogliere le informazioni necessarie (http://support.kaspersky.com/support/details) sul proprio dispositivo e sull'applicazione anti-virus installata. Ciò consentirà ai nostri esperti di assistere l'utente più rapidamente.

GLOSSARIO

A

Aggiornamento

Procedura di sostituzione/aggiunta di nuovi file (database o moduli dell'applicazione) scaricati dai server di aggiornamento di Kaspersky Lab.

Attivazione dell'applicazione

La procedura di attivazione comporta l'immissione del codice di attivazione e la successiva ricezione di un file chiave utilizzato dall'applicazione per determinare i diritti dell'utente e il periodo della licenza.

Archivio

File "contenente" uno o più oggetti che possono essere a loro volta archivi.

B

Blocco di un oggetto

Bloccare dell'accesso a un oggetto da parte di applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

D

Database dell'applicazione

Database creati dagli esperti di Kaspersky Lab, contenenti descrizioni dettagliate di tutte le minacce note per la sicurezza dei computer e i relativi metodi di rilevamento e disinfezione. Questi database vengono costantemente aggiornati da Kaspersky Lab man mano che vengono identificate nuove minacce. Per ottenere una maggiore qualità di rilevamento delle minacce, si consiglia di scaricare regolarmente i database dai server di aggiornamento di Kaspersky Lab.

Disinfezione di oggetti

Metodo utilizzato per elaborare oggetti infetti, che determina il ripristino completo o parziale dei dati o la determinazione che non è possibile disinfettarli. La disinfezione degli oggetti viene eseguita in base al database dell'applicazione. Una parte dei dati validi di un file potrebbe andare persa durante il processo di disinfezione.

E

Eliminazione di un oggetto

Metodo di elaborazione degli oggetti che comporta la loro eliminazione fisica dalle loro posizioni originali (disco rigido, cartella, risorsa di rete). Si consiglia di applicare questo metodo di elaborazione a qualunque oggetto nocivo che non può essere disinfettato.

Eliminazione di un messaggio SMS

Metodo di elaborazione di un messaggio SMS contenente caratteristiche SPAM tali da comportarne la cancellazione. Si raccomanda di utilizzare questo metodo con messaggi SMS contenenti in modo certo spam.

L

Lista bloccati

Le voci contenute in questa lista includono:

- *numeri di telefono* di provenienza delle chiamate e dei messaggi SMS in entrata che verranno bloccate da Anti-Spam, e di destinazione delle chiamate e dei messaggi SMS in uscita che verranno bloccate da Parental Control.
- *testo* che, se contenuto nei messaggi SMS in entrata, ne determinerà il blocco.

LISTA CONSENTITI

Le voci contenute in questa lista includono:

- *numeri di telefono* di provenienza delle chiamate e dei messaggi SMS in entrata che verranno inoltrati da Anti-Spam, e di destinazione delle chiamate e dei messaggi SMS in uscita che verranno inoltrati da Parental Control.

- *testo* che, se contenuto nei messaggi SMS in entrata, ne determinerà l'inoltro.

M

MASCHERA FILE

Rappresentazione del nome e dell'estensione di un file che utilizza i caratteri jolly. I due caratteri jolly principali utilizzati nelle maschere file sono "*****" e "**?**", dove "*****" rappresenta un numero qualsiasi di caratteri e "**?**" sta per qualsiasi carattere singolo. Utilizzando questi caratteri jolly, è possibile rappresentare qualsiasi file. Notare che il nome e l'estensione del file sono sempre separati da un punto.

MITTENTE NON NUMERICO

Numero di telefono che include o è composto unicamente da lettere.

I

OGGETTO INFETTO

Oggetto contenente codice dannoso. L'applicazione rileva gli oggetti infetti eseguendo la scansione del codice binario interno e individua che una sezione del codice dell'oggetto è identica a quella del codice di una minaccia nota. Gli esperti di Kaspersky Lab sconsigliano l'utilizzo di questi oggetti in quanto possono infettare il dispositivo.

L

PERIODO DELLA LICENZA.

Periodo di tempo durante il quale l'utente può utilizzare tute le funzioni dell'applicazione Kaspersky Lab. Di solito, una licenza è valida un anno di calendario dal giorno dell'installazione. Dopo la scadenza della licenza, le funzioni dell'applicazione risulteranno limitate. Non sarà possibile aggiornare i database dell'applicazione.

Q

QUARANTENA

Speciale cartella creata dall'applicazione in cui vengono spostati tutti gli oggetti potenzialmente infetti rilevati dalle scansioni del dispositivo o dal componente Protezione.

R

RIPRISTINO

Il ripristino di un oggetto significa il riposizionamento dell'oggetto originale dalla Quarantena alla cartella originale (in cui si trovava prima di essere messo in quarantena o disinfettato) o in un cartella definita dall'utente.

O

SCANSIONI MANUALI

Modalità di funzionamento dell'applicazione Kaspersky Lab avviata dall'utente e destinata alla scansione di qualsiasi file.

P

TRASFERIMENTO DI OGGETTI IN QUARANTENA

Metodo utilizzato per elaborare un oggetto potenzialmente infetto, che blocca l'accesso a tale oggetto e lo sposta dalla posizione originale alla cartella Quarantena. Nella Quarantena l'oggetto viene memorizzato in forma criptata , il che impedisce l'infezione del dispositivo.

KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è attualmente l'azienda russa leader nello sviluppo di un'ampia gamma di prodotti software ad alte prestazioni per la sicurezza informatica, comprendenti sistemi anti-virus, anti-spam e anti-hacking.

Kaspersky Lab è un'azienda internazionale, con sede centrale nella Federazione Russa e uffici nel Regno Unito, Francia, Germania, Giappone, Benelux, Cina, Polonia, Romania e USA (California). Recentemente è stato aperto in Francia un nuovo ufficio, l'European Anti-Virus Research Centre. La rete di partner di Kaspersky Lab comprende oltre 500 aziende in tutto il mondo.

Attualmente Kaspersky Lab conta oltre mille dipendenti specialisti altamente qualificati, tra cui 10 laureati in economia aziendale e 16 con titolo di PhD. Tutti gli esperti senior in tecnologie anti-virus di Kaspersky Lab sono membri della Computer Anti-Virus Researchers Organization (CARO).

La risorsa più preziosa dell'azienda è l'esclusivo patrimonio di conoscenze e competenze collettive accumulate nel corso di quattordici anni di battaglia ininterrotta contro i virus per computer. L'accurata analisi delle attività dei virus per computer consente agli specialisti dell'azienda di anticipare le tendenze di sviluppo di malware e di fornire agli utenti una protezione tempestiva dai nuovi tipi di attacchi. Questo vantaggio è alla base dei prodotti e dei servizi offerti da Kaspersky Lab. I nostri prodotti sono un passo avanti rispetto a quelli degli altri fornitori nel fornire soluzioni complete di protezione anti-virus ai nostri clienti.

Anni di lavoro intenso hanno reso l'azienda una dei principali sviluppatori di software anti-virus. Kaspersky Lab è stata la prima azienda a sviluppare numerosi standard moderni per la difesa dai virus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus®, fornisce una protezione affidabile per tutti i tipi di computer dagli attacchi di virus, inclusi workstation, file server, sistemi di posta, firewall, gateway Internet e computer palmari. I suoi strumenti di gestione di facile utilizzo consentono un'avanzata automatizzazione della protezione anti-virus per computer e reti aziendali. Numerosi sviluppatori in tutto il mondo utilizzano il kernel di Kaspersky Anti-Virus nei propri prodotti, tra cui Nokia ICG (USA), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

I clienti di Kaspersky Lab possono contare su un'ampia gamma di servizi aggiuntivi che assicurano sia la stabilità operativa dei prodotti dell'azienda che la conformità con requisiti specifici aziendali. Progettiamo, implementiamo e supportiamo sistemi anti-virus di fascia corporate. Il database anti-virus di Kaspersky Lab viene aggiornato ogni ora. L'azienda fornisce ai propri clienti un servizio di assistenza tecnica 24 ore su 24, in varie lingue.

Per domande, commenti o suggerimenti, è possibile contattarci tramite i nostri rivenditori oppure rivolgersi direttamente a Kaspersky Lab. Saremo lieti di assistervi, per telefono o e-mail, su qualunque aspetto relativo ai nostri prodotti. Riceverete risposte complete a tutte le vostre domande.

Sito Web di Kaspersky Lab	http://www.kaspersky.it/
Enciclopedia dei virus:	http://www.viruslist.com
Laboratorio anti-virus:	newvirus@kaspersky.com (solo per l'invio di oggetti sospetti agli archivi) http://support.kaspersky.com/virlab/helpdesk.html?LANG=it (per porre domande agli analisi virus)
Forum Web di Kaspersky Lab:	http://forum.kaspersky.com

CRYPTOEX OOO

Per verificare le firme digitali, Kaspersky Mobile Security utilizza la libreria di software per la sicurezza dei dati Crypto C di CryptoEx OOO.

Sito Web aziendale di CryptoEx OOO: http://www.cryptoex.ru

INDICE

A

Abilitazione
- Anti-Spam ... 52, 140
- Criptaggio ... 93, 182
- Firewall ... 90, 180
- Parental Control ... 64, 152
- Protezione privacy ... 172

Aggiornamento
- avvio manuale ... 98, 188
- avvio pianificato ... 99, 189
- punto di accesso ... 101
- roaming ... 100
- versione dell'applicazione ... 21, 112

Aggiunta
- elenco di contatti protetti di Protezione privacy ... 86, 176
- Lista bloccati Anti-Spam ... 53, 141
- Lista bloccati Parental Control ... 65, 153
- Lista consentiti Anti-Spam ... 56, 145
- Lista consentiti Parental Control ... 68, 157

Antifurto
- SIM Watch ... 77, 166
- SMS-Block ... 72, 161
- SMS-Clean ... 74, 162
- SMS-Find ... 78, 167

Anti-Spam
- azione da eseguire su un messaggio ... 61, 149
- azione da eseguire su una chiamata ... 62, 150
- contatti non in rubrica ... 59, 147
- Lista bloccati ... 53, 141
- Lista consentiti ... 56, 144
- mittenti non numerici ... 60, 148
- modalità ... 52, 140

Archivi
- scansioni manuali ... 47, 133

Attivazione dell'applicazione
- licenza ... 29, 119

Attivazione dell'applicazione ... 22

Attivazione dell'applicazione ... 113

Avvio
- aggiornamento ... 98, 188
- applicazione ... 27, 117
- scansioni manuali ... 41, 130

Azioni
- scansioni manuali ... 45, 135

Azioni da eseguire nei confronti degli oggetti ... 39, 45, 128, 135

B

Blocco
- chiamate in entrata ... 53, 141
- chiamate in uscita ... 65, 153
- connessioni di rete ... 90, 180
- dati codificati ... 95, 184
- messaggi SMS in entrata ... 53, 141
- messaggi SMS in uscita ... 65, 153

Blocco dell'accesso ai dati ... 95, 184

C

Consenti
chiamate in entrata 56, 145
chiamate in uscita 68, 156
connessioni di rete 90, 180
messaggi SMS in entrata 56, 145
messaggi SMS in uscita 68, 156
Contratto di licenza 29, 119
Criptaggio
blocco automatico 95, 184
cripta dei dati 182
Criptaggio dei dati 93
decripta dei dati 94, 183

D

Dati
blocco con codice 95, 184
Criptaggio 93, 182
dati riservati 81, 170
Decripta 183
Decriptaggio 94
Disabilitazione
Anti-Spam 52, 140
Criptaggio 94, 183
Firewall 90, 180
Parental Control 64, 152
Protezione privacy 82, 172
Disinstallazione
applicazione 18, 110

E

Eliminazione
elenco di contatti protetti di Protezione privacy 88, 177
Lista bloccati Anti-Spam 56, 144
Lista bloccati Parental Control 68, 156
Lista consentiti Anti-Spam 59, 147
Lista consentiti Parental Control 71, 159
oggetto dalla quarantena 50, 138
record del report 103, 192

F

File chiave 29, 120
Firewall
livello di sicurezza 90, 180
Firewall
notifica di connessione 91

I

Icona Protezione 33, 107
Installazione dell'applicazione 17, 109
Interfaccia dell'applicazione 33, 123
Invio di un comando 80, 169

L

Licenza 29, 119
attivazione dell'applicazione 22, 113
Contratto di licenza 29, 119
informazioni 30, 121
rinnovo 31, 121

Lista bloccati
Anti-Spam ... 53, 141
Parental Control ... 65, 153
Lista consentiti
Anti-Spam ... 56, 144
Parental Control ... 68, 156
Livello di sicurezza
Firewall ... 90, 180

M

Menu dell'applicazione ... 36, 125
Modalità
Anti-Spam ... 52, 140
Parental Control ... 64, 152
Protezione privacy ... 82, 172
Modifica
elenco di contatti protetti di Protezione privacy ... 87, 176
Lista bloccati Anti-Spam ... 55, 143
Lista bloccati Parental Control ... 67, 155
Lista consentiti Anti-Spam ... 58, 146
Lista consentiti Parental Control ... 70, 158

P

Parental Control
Lista bloccati ... 65, 153
Lista consentiti ... 68, 156
modalità ... 64, 152
Password
codice di attivazione ... 22, 113
password segreta ... 26, 116
password segreta ... 26, 116
Pianifica
aggiornamento ... 99, 189
scansioni manuali ... 43, 132
Protezione privacy
avvio automatico ... 83, 173
avvio remoto ... 84
elenco di contatti protetti ... 86, 175
modalità ... 82
selezione degli oggetti di protezione ... 88, 178

Q

Quarantena
eliminazione di un oggetto ... 50, 138
ripristino di un oggetto ... 50, 137
visualizzazione di oggetti ... 49, 137

R

Report eventi ... 102, 191
eliminazione di voci ... 103, 192
visualizzazione delle voci ... 103, 191
Rete
punto di accesso ... 101
Retroilluminazione ... 106
Rinnovo della licenza ... 31, 121
Ripristino di un oggetto ... 50, 137

S

Scansioni manuali
archivi ... 47

avvio 41, 130
avvio pianificato 43, 132
azioni da eseguire sugli oggetti 45, 135
oggetti da sottoporre a scansione 44, 133
Schede dell'applicazione 35
Segnale acustico 105
Stato di protezione 34, 106, 123

V

Visualizzazione
finestra Stato di protezione 34, 123
icona Protezione 33, 107
retroilluminazione 106
Voce
Lista bloccati Anti-Spam 53, 141
Lista consentiti Anti-Spam 56, 145
Lista consentiti Parental Control 68, 157